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

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 Steven Hernandez - CISSP, CAP, SSCP, CSSLP

(ISC)²®

THIRD EDITION

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

THIRD EDITION

OTHER BOOKS IN THE (ISC)²® PRESS SERIES

Official (ISC)²® Guide to the CISSP® CBK®, Third Edition
Harold F. Tipton, Editor
ISBN: 978-1-4665-6976-8

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®

THIRD EDITION

Edited by
Steven Hernandez - CISSP, CAP, SSCP, CSSLP

(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

© 2012 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20130315

International Standard Book Number-13: 978-1-4665-6978-2 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

Foreword xv
Introduction xviii
Editors xxx
Contributors xxxiv

DOMAIN 1
ACCESS CONTROL

Key Access Control Concepts 4
ACCESS CONTROL PRINCIPLES 17
TYPES & CATEGORIES OF ACCESS CONTROLS 44
ACCESS CONTROL TYPES 53
ACCESS CONTROL TECHNIQUES 81
IDENTIFICATION AND AUTHENTICATION 94
DECENTRALIZED/DISTRIBUTED ACCESS CONTROL TECHNIQUES 149
LOGGING AND MONITORING 175
Access Control Attacks 194
UNDERSTANDING THREATS 194
THREAT MODELING 227
ASSET VALUATION 230
ACCESS AGGREGATION 234

Assess Effectiveness of Access Controls 235
USER ENTITLEMENT 252
ACCESS REVIEW & AUDIT 253
Identity and Access Provisioning Lifecycle 256

DOMAIN 2
SECURITY NETWORK ARCHITECTURE & DESIGN

Secure Network Architecture and Design 271
OSI and TCP/IP 273
IP NETWORKING 288
IMPLICATIONS OF MULTI-LAYER PROTOCOLS 312
Securing Network Components 316
HARDWARE 321
TRANSMISSION MEDIA 328
NETWORK ACCESS CONTROL DEVICES 347
END-POINT SECURITY 354
Secure Communication Channels 355
VOICE 364
MULTIMEDIA COLLABORATION 371
REMOTE ACCESS 381
DATA COMMUNICATIONS 388
Network Attacks 416

DOMAIN 3
INFORMATION SECURITY GOVERNANCE & RISK MANAGEMENT

Understand and Align Security Function 467
Understand and Apply Security Governance 470
ORGANIZATIONAL PROCESSES 473
SECURITY ROLES AND RESPONSIBILITIES 475

LEGISLATIVE AND REGULATORY COMPLIANCE 482
PRIVACY REQUIREMENTS COMPLIANCE 484
CONTROL FRAMEWORKS 485
DUE CARE 487
DUE DILIGENCE 488
Concepts of Confidentiality, Integrity and Availability 489
Develop and Implement Security Policy 492
SECURITY POLICIES 495
STANDARDS/BASELINES 500
PROCEDURES 503
GUIDELINES 504
DOCUMENTATION 505
Manage the Information Life Cycle 507
Manage Third-Party Governance 510
Understand and Apply Risk Management Concepts 512
QUANTITATIVE RISK ASSESSMENTS 527
IDENTIFY THREATS AND VULNERABILITIES 529
RISK ASSESSMENT/ANALYSIS 532
RISK ASSIGNMENT/ACCEPTANCE 538
COUNTERMEASURE SELECTION 541
TANGIBLE AND INTANGIBLE ASSET VALUATION 543
Manage Personnel Security 547
EMPLOYMENT CANDIDATE SCREENING 548
EMPLOYMENT AGREEMENTS AND POLICIES 557
EMPLOYEE TERMINATION PROCESSES 562
VENDOR, CONSULTANT AND CONTRACTOR CONTROLS 564
Security Education, Training and Awareness 566
Manage the Security Function 574
BUDGET 588
METRICS 590
RESOURCES 591

DEVELOP AND IMPLEMENT INFORMATION SECURITY STRATEGIES 593
EFFECTIVENESS OF THE SECURITY PROGRAM 596

DOMAIN 4
SOFTWARE DEVELOPMENT SECURITY

Security in the Software Development Life Cycle 614
DEVELOPMENT LIFE CYCLE 618
MATURITY MODELS 626
OPERATION AND MAINTENANCE 629
CHANGE MANAGEMENT 630
Environment and Security Controls 632
SECURITY OF THE SOFTWARE ENVIRONMENT 676
SECURITY ISSUES OF PROGRAMMING LANGUAGES 681
SECURITY ISSUES IN SOURCE CODE 699
CONFIGURATION MANAGEMENT 747
Assess the Effectiveness of Software Security 748

DOMAIN 5
CRYPTOGRAPHY

The Application and Use of Cryptography 764
DATA AT REST 771
DATA IN TRANSIT 771
THE CRYPTOGRAPHIC LIFECYCLE 773
ENCRYPTION CONCEPTS 778
SYMMETRIC CRYPTOGRAPHY 801
ASYMMETRIC CRYPTOGRAPHY 822
HYBRID CRYPTOGRAPHY 829
MESSAGE DIGESTS 831
HASHING 832
Key Management Processes 838
CREATION AND DISTRIBUTION OF KEYS 848

KEY STORAGE AND DESTRUCTION 855
KEY RECOVERY 860
KEY ESCROW 860
Digital Signatures 862
Non-Repudiation 865
Methods of Cryptanalytic Attacks 866
CHOSEN PLAIN-TEXT 866
SOCIAL ENGINEERING FOR KEY DISCOVERY 866
BRUTE FORCE 866
CIPHERTEXT-ONLY ATTACK 868
KNOW PLAINTEXT 869
FREQUENCY ANALYSIS 869
CHOSEN CIPHER-TEXT 869
IMPLEMENTATION ATTACKS 871
NETWORK SECURITY AND CRYPTOGRAPHY 873
APPLICATION SECURITY AND CRYPTOGRAPHY 876
PUBLIC KEY INFRASTRUCTURE (PKI) 879
CERTIFICATE RELATED ISSUES 882
INFORMATION HIDING ALTERNATIVES 885

DOMAIN 6
SECURITY ARCHITECTURE & DESIGN

Fundamental Concepts of Security Models 902
Information Systems Security Evaluation Models 945
PRODUCT EVALUATION MODELS 948
INDUSTRY AND INTERNATIONAL SECURITY IMPLEMENTATION GUIDELINES 956
Security Capabilities of Information Systems 963
VULNERABILITIES OF SECURITY ARCHITECTURES 970
SYSTEM 970
TECHNOLOGY AND PROCESS INTEGRATION 974

Software and System Vulnerabilities and Threats 979
WEB-BASED 979
CLIENT-BASED VULNERABILITIES 983
SERVER-BASED VULNERABILITIES 986
DATABASE SECURITY 989
DISTRIBUTED SYSTEMS 992
Countermeasure Principles 999

DOMAIN 7
SECURITY OPERATIONS

Security Operations Concepts 1014
NEED TO-KNOW/LEAST PRIVILEGE 1017
SEPARATION OF DUTIES AND RESPONSIBILITIES 1021
MONITOR SPECIAL PRIVILEGES 1026
JOB ROTATION 1027
MARKING, HANDLING, STORING AND DESTROYING OF SENSITIVE INFORMATION 1027
RECORD RETENTION 1031
Employ Resource Protection 1032
MEDIA MANAGEMENT 1035
ASSET MANAGEMENT 1041
Manage Incident Response 1043
DETECTION 1047
RESPONSE 1051
REPORTING 1052
RECOVERY 1052
REMEDIATION AND REVIEW 1053

Preventative Measure against Attacks 1056
Patch and Vulnerability Management 1058
Change and Configuration Management 1063
System Resilience/Fault Tolerance Requirements 1068

DOMAIN 8
BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING

Business Continuity Requirements 1092
DEVELOP AND DOCUMENT PROJECT SCOPE AND PLAN 1095
Conduct Business Impact Analysis 1108
IDENTIFY AND PRIORITIZE CRITICAL ORGANIZATION FUNCTIONS 1108
DETERMINE MAXIMUM TOLERABLE DOWNTIME AND OTHER CRITERIA 1110
ASSESS EXPOSURE TO OUTAGES 1111
DEFINE RECOVERY OBJECTIVES 1115
Develop a Recovery Strategy 1117
IMPLEMENT A BACKUP STORAGE STRATEGY 1118
RECOVERY SITE STRATEGIES 1121
The Disaster Recovery Process 1127
RESPONSE 1129
PERSONNEL 1135
COMMUNICATIONS 1136
ASSESSMENT 1138
RESTORATION 1139
PROVIDE TRAINING 1141
Exercise, Assess and Maintain the Plan 1143

DOMAIN 9
LEGAL, REGULATIONS, INVESTIGATIONS, AND COMPLIANCE

Legal Issues Internationally 1168
COMPUTER CRIME 1176
LICENSING AND INTELLECTUAL PROPERTY 1180
IMPORT/EXPORT 1184
TRANS-BORDER DATA FLOW 1184
PRIVACY 1184
Understand Professional Ethics 1193
(ISC)² CODE OF PROFESSIONAL ETHICS 1208
SUPPORT ORGANIZATION'S CODE OF ETHICS 1210
Understand and Support Investigations 1217
POLICY, ROLES AND RESPONSIBILITIES 1223
INCIDENT HANDLING AND RESPONSE 1225
EVIDENCE COLLECTION AND HANDLING 1232
REPORTING AND DOCUMENTING 1234
Understand Forensic Procedures 1235
MEDIA ANALYSIS 1236
NETWORK ANALYSIS 1236
SOFTWARE ANALYSIS 1237
HARDWARE/EMBEDDED DEVICE ANALYSIS 1238
Understand Compliance Requirements and Procedures 1240
REGULATORY ENVIRONMENT 1240
AUDITS 1240
REPORTING 1241
Contractual Agreements and Procurement Processes 1242

DOMAIN 10
PHYSICAL (ENVIRONMENTAL) SECURITY

Understand Site and Facility Design Considerations 1256

Support the Implementation and Operation of Perimeter Security 1275

Support the Implementation of Internal Security 1308

Support the Implementation and Operation of Facilities Security 1331

COMMUNICATIONS AND SERVER ROOMS 1337

RESTRICTED AND WORK AREA SECURITY 1339

DATA CENTER SECURITY 1340

UTILITIES AND HVAC CONSIDERATIONS 1343

WATER ISSUES 1347

FIRE PREVENTION, DETECTION AND SUPPRESSION 1347

Support the Protection and Securing of Equipment 1351

Personnel Privacy and Safety 1357

APPENDIX
ANSWERS TO REVIEW QUESTIONS

DOMAIN 1 *- ACCESS CONTROL* 1371

DOMAIN 2 *- TELECOMMUNICATIONS AND NETWORK SECURITY* 1379

DOMAIN 3 *- INFORMATION SECURITY GOVERNANCE AND RISK* 1387

DOMAIN 4 *- SOFTWARE DEVELOPMENT SECURITY* 1395

DOMAIN 5 *- CRYPTOGRAPHY* 1406

DOMAIN 6 *- SECURITY ARCHITECTURE AND DESIGN* 1412

DOMAIN 7 *- SECURITY OPERATIONS* 1422

DOMAIN 8 *- BUSINESS CONTINUITY & DISASTER RECOVERY PLANNING* 1431

DOMAIN 9 *- LEGAL, REGULATIONS, INVESTIGATIONS, AND COMPLIANCE* 1439

DOMAIN 10 *- PHYSICAL (ENVIRONMENTAL) SECURITY* 1445

Foreword

Foreword to CISSP CBK Study Guide - Third Edition

We are living in an advanced cyber era, with every aspect of our lives, from medical records to bank transactions, now being transmitted online. The plethora of data and information flooding cyber space is overwhelming and there simply aren't enough qualified information security professionals to protect it all.

(ISC)²'s mission is to support and provide members and constituents with credentials, resources, and leadership to secure information and deliver value to society. The not-for-profit, vendor-neutral organization was founded by a group of passionate volunteers in 1989 who wanted to create an information security industry standard for professionals. Their initial concept for industry excellence came to fruition with the creation of the Certified Information Systems Security Professional (CISSP®) credential. It was the first technology-related credential to be accredited by the International Organization for Standardizations (ISO) ISO/IEC Standard 17024, a global benchmark for the certification of personnel.

The CISSP continues to be recognized as the industry's Gold Standard. The true differentiator is the organization's stringent membership requirements – passing the examination, possessing the required number of years of in depth experience in at least 2 of the domains, being endorsed

by another (ISC)² member in good standing, abiding by a Code of Ethics, and maintaining quality continuing professional education (CPE) credits.

The CISSP is not only recognized throughout the industry, it's also highly regarded by governments, academia, human resources, and business entities around the world. In fact, the CISSP has become a job requirement and/or candidate differentiator for information security management positions.

The ten domains of the CISSP CBK® comprehensively encompass the core competencies that an experienced information security professional should possess. The latest security topics such as cloud computing, mobile security, application security, and more are regularly integrated into the examination through a rigorous process of evaluation and updates. We require our members to obtain the industry's latest knowledge and skills, and we reinforce that sentiment through our own examination process.

83% of (ISC)² members are employed in a wide variety of technically diverse professions and 17% are employed in governance and policy making roles.

The Official (ISC)² Guide to the CISSP CBK is the only study tool that delves into all of the topics and subtopics contained in the CISSP CBK. The authors and editor of this new, comprehensive edition have provided an extensive supplement to the CBK review seminars that are designed to help candidates study for the CISSP credential.

Earning the CISSP is a major highlight in an information security professional's career path. (ISC)²'s elite network of professionals enjoy benefits such as: complimentary access to (ISC)²'s one-day conferences and networking receptions in cities around the world; discounts at industry conferences; access to a Career Center with current job listings; subscription to (ISC)²'s digital magazine – InfoSecurity Professional; a dedicated member services staff to address your questions and issues; and much more.

You will also be a member of a highly respected organization that is dedicated to reaching society and shaping the industry at large through community goodwill programs such as Safe and Secure Online, academic scholarships for students, and cutting-edge research –under the (ISC)^2 Foundation.

We wish you success in your journey to becoming a CISSP.

W. Hord Tipton
International Information System Security Certification Consortium, Inc.

Introduction

The Certified Information Systems Security Professional (CISSP) is an information assurance professional who has demonstrated a cross-disciplinary expertise ranging from architecture, design, management, risk and controls that assure the security of business environments. 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 10 domains of the (ISC)² CISSP CBK. A firm understanding of what the 10 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 10 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.

While there is a strong interaction amongst the ten domains of the CISSP, security mechanisms are covered in Access Control, Software Development Security, Cryptography, the Physical (Environmental) Security, and the Telecommunications and Network Security domains. Security policies are addressed in the Security Architecture & Design, the Information Security Governance and Risk Management, The Business Continuity and Disaster Recovery Planning and Security Operations domains. The people aspects of security encompass a cross section of domains, and are specifically covered in the Legal, Regulations, Investigations and Compliance domain.

1. The ***Access Control*** domain covers mechanisms by which a system grants or revokes the right to access data or perform an action on an information system.

Access Control systems include:

- File permissions, such as "create," "read," "edit," or "delete" on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data rights, such as the right to retrieve or update information in a database.

These elements of Access Control systems are things that Information Security professionals interact with every day, as do the users of any systems that the business provides, such as Directory Services for logon authentication, File and Print systems that allow for the secure storage, retrieval, and manipulation of data in a variety of formats, as well as web services that expose data to front end interfaces for user consumption. Whenever a user attempts to access secured data from any legitimate or illegitimate interface, internal or external to the enterprise, the Access Control domain plays an active and indispensable part in the transactions that take place to ultimately either validate, or disqualify that user's access request. The ability to understand Identity Management, Data Access Controls, Information Classification, System Access Control Strategies, and Threats, are all key elements that go into the Access Control Domain.

2. The ***Telecommunications and Network Security*** domain encompasses the structures, techniques, transport protocols, and security measures used to provide integrity, availability, confidentiality and authentication for transmissions over private and public communication networks.

The Information Security professional is responsible for security at all levels of the business, whether it is with regards to a senior level executive's

request to access controlled information, or the testing and deployment of an application security patch, or the documentation of the processes and procedures that are in place to safeguard remote access to the business's data. Identification of threat and risk, and the implementation of mitigation techniques and strategies to counteract and minimize their impacts also play an important part in the list of activities that the Information Security professional is responsible for carrying out and managing on a daily basis within the business. All of these things are part of the Telecommunications and Network Security domain in one way or another. The 7 layers of the OSI model that are used to describe the activities and structure of the network, and how information is structured, transmitted, formatted, and secured with a focus on providing for Confidentiality, Integrity, and Availability (CIA) are the roadmap for the Information Security professional in this domain, allowing them to understand at **ALL** levels of a system, from end to end, how to envision information and the security that needs to envelop it to ensure it is properly protected and safeguarded.

3. The ***Information Security Governance and Risk Management*** domain entails the identification of an organization's information assets and the development, documentation, implementation and updating of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.

The Information Security professional is actively involved in all aspects of the Information and Security Governance and Risk Management domain as part of any of the functions that they carry out within the enterprise. Whether it is the creation of compelling business cases for senior management to illustrate the Core Information Security Principles of Confidentiality, Availability, and Integrity (CIA) inherent in a current business system, or new software platform, or the clear delineation of the required Security

Policies, Procedures, Standards, Guidelines, and Baselines needed to run and maintain current systems, as well as testing new systems and software for possible deployment and use, the Information Security professional actively champions the Information Security Governance and Risk Management domain in all that they do within the business. The Information Security professional is also responsible for ensuring that the business, and all of its users are acting ethically with regards to information management and security, and that any and all activities engaged in always safeguard people first, as well as safeguarding the information that they are accessing.

4. The ***Software Development Security*** domain refers to the controls that are included within systems and applications software and the steps used in their development, for example a Software Development Life Cycle (SDLC).

Software refers to system software (operating systems) and application programs such as agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

The elements of Software Development Security are not the direct purview of many Information Security professionals. Software development is a highly specialized skill, and most Information Security professionals are not software developers traditionally. As a result, on the surface it may appear to Information Security professionals as if they cannot be effective in this domain of the CBK, but nothing can be further from the truth. Software forms the working foundation of every system that the Information Security professional and users in any business anywhere in the world interact with on a daily basis. While users typically do not understand the answer to the question of "how" their software was created, they do understand how to use that software, but unfortunately, not always in a secure and responsible manner. Being able to provide guidance to users with regards to things such as Malicious Software types and identification,

Audit and Assurance Mechanisms, Database Controls, and Web Application Threats are all elements that the Information Security professional will put in place as part of the Software Development and Security domain.

5. The ***Cryptography*** domain addresses the principles, means, and methods of applying mathematical algorithms and data transformations to information to ensure its integrity, confidentiality and authenticity.

While many of the physical elements of the Cryptography domain are used by business all the time to safeguard data and to ensure data integrity, most users are unaware of these functions and how they operate. Whether it is the use of Symmetric or Asymmetric Cryptography to protect data and ensure confidentiality, or the use of Hash Functions or Digital Signatures to ensure message integrity, or the practice of Encryption Management to ensure data availability on demand for authenticated users of a system, the Information Security professional plays an active role in all aspects of the Cryptography domain, and its application to data security in the enterprise. The other components of the Cryptography domain, such as the concepts of Nonrepudiation, Authentication, and Access Control are also important areas that the Information Security professional will actively be involved with as they set up and manage Directory Service based authentication systems such as Active Directory, or Network Information Service (NIS) systems, as well as encryption key management solutions.

6. The ***Security Architecture & Design*** 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.

The Information Security professional needs to remember that they are charged with providing direction and guidance to the business and its users in the various areas of the CISSP CBK. The best way for them to be able to accomplish that goal consistently, across all of the 10 domains of the CBK, is to be aware of the actions and activities that they already engage in everyday that align with the CBK, and allow them to translate the CBK into tangible action and measurable results for the business and its users. The Security Architecture & Design domain is all about the What, Why and How of security. The Information Security professional needs to be able to use these questions to examine the needs of the business and its users for secure access to information, and then to develop systems that will foster the level of secure access required. Measurement of that system and ongoing maintenance of it is addressed through other domains of the CISSP CBK, but the foundation necessary to ensure success of those efforts is built by the Information Security professional as they create well-formed and sound Security Architectures and Designs.

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 ***Business Continuity and Disaster Recovery Planning*** domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures.

The Information Security professional may or may not have direct experience with an actual disaster and the recovery actions that would be necessary to bring the business back to full functionality, while ensuring the safety and integrity of the business systems and information, as well as the safety and well- being of the users in the systems. Whether the Information Security professional has this direct, first- hand experience of applying a BCP and/or a DRP to an actual event is not as critical as their knowledge of, and training in the specific processes and procedures that are in place for their business in the event of an emergency, or an event that will negatively impact the business and its users. In addition, solid grounding in Project Management skills and the ability to interface with other risk management areas such as records management, regulatory compliance, vendor management, and physical security in the context of a Risk Management Framework that is used to help all areas of the business respond to and deal with risk effectively is also a critical success factor for the Information Security professional.

Business Continuity Planning (BCP) helps to identify the organization's exposure to internal and external threats. BCP counteracts interruptions to business activities and should be available to protect critical business processes from the effects of major failures or disasters. It deals with the natural and man-made events and the consequences, if not dealt with promptly and effectively.

Business Impact Analysis (BIA) determines the proportion of impact an individual business unit would sustain subsequent to a significant interruption of computing or telecommunication services. These impacts may be financial, in terms of monetary loss, or operational, in terms of inability to deliver.

Disaster Recovery Plans (DRP) contain procedures for emergency response, extended backup operation and post-disaster recovery, should a computer installation experience a partial or total loss of computer resources and physical facilities. The primary objective of the disaster recovery plan is to provide the capability to process mission-essential applications, in a degraded mode, and return to normal mode of operation within a reasonable amount of time.

9. The ***Legal, Regulations, Investigations and Compliance*** domain addresses ethical behavior and compliance with regulatory frameworks. It includes the investigative measures and techniques that can be used to determine if a crime has been committed, and methods used to gather evidence (e.g., forensics). A computer crime is any illegal action where the data on a computer is accessed without permission. This includes unauthorized access or alteration of data, or unlawful use of computers and services. This domain also includes understanding the computer incident forensic response capability to identify the Advanced Persistent Threat (APT) that many organizations face today.

Information Security professionals operate in a variety of environments today, and as a result of this diversity, they must be aware of any and all

legal and regulatory responsibilities that the business may be subject to with regards to computer crime, data access, data use, data manipulation, and unauthorized data destruction. Understanding how to organize the response of the business to a computer incident, and to be able to interface with any and all other areas of Risk Management and Information Security Management as required to coordinate the response and ongoing communication and coordination efforts of the business with regards to the forensic examination of evidence are important functions that the Information Security professional should be comfortable with.

10. The ***Physical (Environmental) Security*** domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts.

The Information Security professional should be exercising a "holistic" vision of the business and its resources when it comes to security. Taking into account both the physical and logical aspects of security design, as well as the entirety of the business's physical footprint, are all important elements of success for the Information Security professional to be measuring their approaches and actions against with regards to the Physical (Environmental) Security domain. While many Information Security professionals will not be involved with the initial site and facility design criteria, and even the location choices for the business that they are a part of, that does not mean that they should not be aware of these factors with regards to their impact on security. Further, Information Security professionals need to play an active part in creating a focus within the

business on the efficacy of its physical security posture, and if necessary, to be the agent that drives changes as required to ensure that security is maintained at appropriate levels given the threats and risks that are present in the operating environment.

Editors

Steven Hernandez - Lead Editor

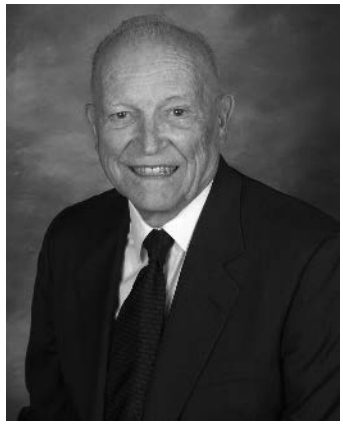
Steven Hernandez MBA, CISSP, CSSLP, SSCP, CAP, CISA is the Chief Information Security Officer and the Director of Information Assurance for the Office of Inspector General at the US Department of Health and Human Services. Hernandez has over seventeen years of information assurance experience in a variety of fields including international heavy manufacturing, large finance organizations, educational institutions, and Government agencies. Steven is affiliate faculty at the National Information Assurance Training and Education Center located at Idaho State University. Through his academic outreach, he has presented lectures over the past decade on numerous information assurance topics including risk management, information security investing, and the implications of privacy decisions to graduate and post graduate audiences. In addition to his credentials from (ISC)^2, Hernandez also holds six US 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. When not engaged in information assurance pursuits he enjoys relaxing with his family and their overly demanding dog.

Adam Gordon - Technical Editor

With over 20 years of experience as both an educator and IT professional, Adam holds numerous Professional IT Certifications including CISA, CISSP, CRISC, CHFI, CEH, SCNA, VCP, and VCI. He is the author of several books and has achieved many awards, including EC-Council Instructor of Excellence for 2006-07 and Top Technical Instructor Worldwide, 2002-2003. 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.



In Memoriam

Harold F. (Hal) Tipton - Original Editor

Hal Tipton, was a past president of the International Information System Security Certification Consortium and a director of computer security for Rockwell International Corporation for about 15 years. He initiated the Rockwell computer and data security program in 1977 and then continued to

administer, develop, enhance, and expand the program to accommodate the control needs produced by technological advances until his retirement from Rockwell in 1994.

Tipton was a member of the Information Systems Security Association (ISSA) since 1982 and became the president of the Los Angeles Chapter in 1984, and the president of the national organization of ISSA (1987–1989). He was added to the ISSA Hall of Fame and the ISSA Honor Role in 2000.

Tipton was a member of the National Institute for Standards and Technology (NIST), the computer and Telecommunications Security Council, and the National Research Council Secure Systems Study Committee (for the National Academy of Science). He received his BS in engineering from the U.S. Naval Academy and his MA in personnel administration from George Washington University; he also received his certificate in computer science from the University of California at Irvine. He was a certified information system security professional (CISSP), ISSAP, & ISSMP.

He last chaired the (ISC)^2 CBK Committees and the QA Committee and received the Computer Security Institute's Lifetime Achievement Award in 1994 and the (ISC)^2's Hal Tipton Award in 2001. As important as he was to the field of Information Systems Security, he was an even better man. Hal will be missed as a leader, visionary, pioneer, and most importantly – a great friend by all that had the honor to get to know him.

Contributors

Paul Baker, Ph.D., CPP, is a security manager with more than 30 years of extensive and comprehensive experience in all phases of law enforcement and industrial security. He holds a doctorate in strategic leadership from Regent University along with a master of science in criminal justice from Troy University. Dr. Baker began his security management journey in the U.S. Marine Corps and continued as a Maryland State Trooper working extensively on narcotics and intelligence. After his retirement in 2001, he embarked on the next phase of his security career, working as a physical security supervisor for the MITRE Corporation in Washington, D.C. He is currently employed as a security manager for Capital One Bank. Dr. Baker has been involved in numerous security assessment projects and has designed complete physical protection systems for a multitude of facilities.

Alec Bass, CISSP, is a senior security specialist in the Boston area. During his 25 year career, Alec has developed solutions that significantly reduce risk to the digital assets of high-profile manufacturing, communications, home entertainment, financial, research, and federal organizations. He has helped enterprises enhance their network's security posture, performed penetration testing, and administered client firewalls for an application service provider. Before devoting his career to information security, Alec supported the IT infrastructure for a multinational Fortune 200 company and fixed operating system bugs for a leading computer firm.

Peter Berlich, CISSP-ISSMP, is working as an IT security manager on a large outsourcing account at IBM Integrated Technology Services, coming from a progression of IT security- and compliance-related roles in IBM. Before joining IBM, he was global information security manager at ABB, after a succession of technical and project management roles with a focus on network security management. Peter is a member of the (ISC)² European Advisory Board and the Information Security Forum Council. He is the author of various articles on the subject of security and privacy management in publications such as *Infosecurity Today*.

Todd Fitzgerald, CISSP, CISA, CISM, is the director of information systems security and a systems security officer for United Government Services, LLC (UGS), Milwaukee, Wisconsin. Todd has written articles on information security for publications such as The Information Security Management Handbook, The HIPAA Program Reference Book, Managing an Information Security and Privacy Awareness and Training Program (Auerbach Publications) and magazines such as Information Security. Todd is frequently called upon to present at national and local conferences, and has received several security industry leadership awards.

Stephen Fried, CISSP, CISM, is a seasoned information security professional with over 25 years' experience in information technology. For the last 12 years, Stephen has concentrated his eff orts on providing effective information security leadership to large organizations. Stephen has led the creation of security programs for two Fortune 500 companies and has an extensive background in such diverse security issues as risk assessment and management, security policy development, security architecture, infrastructure and perimeter security design, outsource relationship security, off shore development, intellectual property protection, security technology development, business continuity, secure e-business design, and information technology auditing. A frequent speaker at conferences, Stephen is also active in many security industry organizations. He is a contributing author to the Information Security Management Handbook, and has also been quoted in magazines such as Secure Enterprise and CIO Decisions.

Bonnie A. Goins, CISSP, NSA IAM, GIAC, CISM, ISS, PCI QSA, is a nationally recognized subject matter expert in information security management. With over 17 years of experience in management consulting, and information technology and security, Bonnie is chosen by executive management for her depth of knowledge and experience in information technology and security strategy development and refinement; risk and security assessment methods; security program design, development, and implementation; regulatory compliance initiatives, such as HIPAA, Sarbanes–Oxley, PCI, GLBA, NERC/FERC, FISMA, and others; policy, procedure, and plan creation; technology and business process reengineering; secure network infrastructure design and implementation; business continuity and incident response initiatives; application security methods; and security/technology/regulatory training. Her experience extends over multiple verticals and includes healthcare, financial services, government, utilities, retail, higher education, telecommunications, manufacturing, public health, pharmaceuticals/biotech, and manufacturing.

Kevin Henry, CISSP-ISSEP, ISSMP, CAP, SSCP, is a well-known speaker and consultant in the fi eld of information security and business continuity planning. He provides educational and consulting services to organizations throughout the world and is an official instructor for $(ISC)^2$. He is responsible for course development and delivery for several $(ISC)^2$ programs. Kevin has a broad range of experience in both technology and management of information technology and information security programs. He has worked for clients ranging from the largest telecommunications firms in the world to governments, military, and small home-based operations. He is a highly respected presenter at conferences, seminars, and educational programs worldwide. With over 20 years of telecommunications and government experience, he brings a relevant and interesting approach to information security and provides practical and meaningful solutions to the information security challenges, threats, and regulations we face today.

Rebecca Herold, CISSP, CISM, CISA, FLMI, is an information privacy, security, and compliance consultant, author, and instructor with over

16 years of experience assisting organizations of all sizes in all industries throughout the world. Rebecca has written numerous books, including Managing an Information Security and Privacy Awareness and Training Program (Auerbach Publications) and The Privacy Management Toolkit (Information Shield), along with dozens of book chapters and hundreds of published articles. Rebecca speaks often at conferences, and develops and teaches workshops for the Computer Security Institute. Rebecca is a resident editor for the IT Compliance Community and also an adjunct professor for the Norwich University Master of Science in information assurance program.

Micki Krause, CISSP, has held positions in the information security profession for the last 20 years. She is currently the chief information security officer at Pacific Life Insurance Company in Newport Beach, California. Micki has held several leadership roles in industry-influential groups including the ISSA and the (ISC)² and is a long-term advocate for professional security education and certification. In 2003, Krause received industry recognition as a recipient of the "Women of Vision" award given by Information Security magazine. In 2002, Krause was honored as the second recipient of the Harold F. Tipton Award in recognition of sustained career excellence and outstanding contributions to the profession. She is a reputed speaker, published author, and coeditor of the Information Security Management Handbook series.

Tyson Macaulay, the security liaison officer for Bell Canada, is responsible for technical and operational risk management solutions for Bell's largest enterprise clients. Tyson leads security initiatives addressing large, complex, technology solutions including physical and logical (IT) assets, and regulatory/legal compliance requirements. In this role, he leads worldwide engagements involving multinational companies and international governments. Tyson's leadership encompasses a broad range of industry sectors from the defense industry to high-tech start-ups. His expertise includes large-scale security implementations in both public and private sector institutions, working on projects from conception through

development to implementation. Tyson is a respected thought leader with publications dating from 1993. His work has covered authorship of peer-reviewed white papers, IT security governance programs, technical and integration services, and incident management processes.

Kelley Okolita, MBCP, is currently the program manager for business continuity and disaster recovery for the Hanover Insurance Group. Widely recognized as an industry expert with more than 25 years' experience, Kelley developed and implemented programs that were put to the test and proved successful for a variety of recoveries both large and small including from the events of September 11, 2001 and Hurricane Katrina. Kelley is sought after as a speaker and subject-matter expert by organizations such as Gartner, Sungard, and IBM. She has published articles in professional magazines and journals and was selected by $(ISC)^2$ to be the expert to rewrite Chapter 3 for their CISSP study guide and ISSAP study guide. Kelley has had a 10-year affiliation with DRI International (DRII)—six years on the Certification Commission for DRII, two as a chair and two as a member of their board of directors. She continues to serve on various committees. She is also an alternate on the NFPA 1600 Technical Committee. She has spoken at conferences from North America to Australia to Singapore and is currently completing her book on enterprise-wide business continuity planning, which is to be published by Taylor & Francis.

Keith Pasley, CISSP, CISA, ITIL, GSNA, is an information security professional specializing in helping companies understand information security requirements, regulatory compliance to help maximize security technology to reduce costs and complexity. Keith has over 20 years of hands-on experience in the information technology industry, and has spent the last 13 years specializing in information security. In various roles, Keith has designed security architectures and implemented security strategies for government, education, and commercial sectors. Keith is a security researcher and a contributing author to such publications as the Information Security Management Handbook and the HIPAA Program Reference (both published by Auerbach Publications). Keith has also

published online and in-print articles on various security-related subjects.

Marcus K. Rogers, Ph.D, CISSP, CCCI, is the director of the Cyber Forensics Program in the Department of Computer and Information Technology at Purdue University. He is a professor, a faculty scholar, and a research faculty member at the Center for Education and Research in Information Assurance and Security. Dr. Rogers is a member of the quality assurance board for (ISC)²'s SCCP designation; the international chair of the Law, Regulations, Compliance and Investigation Domain of the Common Body of Knowledge (CBK) committee; the chair of the Ethics Committee Digital & Multimedia Sciences Section—American Academy of Forensic Sciences; and the chair of the Certification Committee Digital Forensics Certification Board. Dr. Rogers is the editor in chief of the Journal of Digital Forensic Practice and serves on the editorial board of several other professional journals. He is the author of numerous book chapters and journal publications in the field of digital forensics and applied psychological analysis.

Ken M. Shaurette, CISSP, CISA, CISM, is an experienced security and audit professional with a strong understanding of complex computing environments, legislative and regulatory requirements, and security solutions. He is a founding member and a past president of the Western Wisconsin InfraGard Chapter; a past president of ISSA-Milwaukee (International Systems Security Association); the current president and founding member of ISSA-Madison; a past chairman MATC Milwaukee Security Specialist Curriculum Advisory Committee; a member of Herzing University's Department of Homeland Security Degree; and a member of the Western Wisconsin Association of Computer Crime Investigators. Ken has published security information in several books and trade magazines. In his spare time, he finds time to work as a director of IT services for Financial Institution Products Corporation (FIPCO®), a subsidiary of the Wisconsin Bankers Association. He can be reached via e-mail at kshaurette@charter.net.

Robert M. Slade is an information security and management consultant from North Vancouver, British Columbia, Canada. Initial research into computer viral programs developed into the writing and reviewing of security books, and eventually into conducting review seminars for CISSP candidates. Slade also promotes the Community Security Education project, attempting to increase security awareness for the general public as a means of reducing overall information security threats. More information than anyone would want to know about him is available at http://victoria.tc.ca/techrev/rms.htm or http://en.wikipedia.org/wiki/Robert_Slade. It is next to impossible to get him to take "bio" writing seriously.

James S. Tiller, CISSP, CISA, is an accomplished executive with over 14 years of information security and information technology experience and leadership. He has provided comprehensive, forward-thinking solutions encompassing a broad spectrum of challenges and industries. Jim has spent much of his career assisting organizations throughout North America, Europe, and most recently Asia, in meeting their security goals and objectives. He is the author of Th e Ethical Hack: Framework for Business Value Penetration Testing and A Technical Guide to IPsec Virtual Private Networks (Auerbach Publications). Jim has been a contributing author to the Information Security Management Handbook for the last five years, in addition to several other publications. Currently, Jim is the vice president of Security North America for BT Global Services.

Additional images, tables, illustrations and grammatical edits provided by ***Andrew Schneiter.***

Additional illustrations by ***Andrea Graves***.

Domain 1

Access Controls

THE FIELD OF INFORMATION SECURITY is complex, dynamic, and infinitely challenging. This single discipline contains elements of advanced technology, human behavior, business strategy, statistical analysis, mathematics, and a host of other technical and personal skills. In fact, the field can be so complex that to categorize it for the CBK® takes ten distinct domains, each with its own unique skill and knowledge requirements. Despite all this complexity, however, the fundamental purpose of all information security efforts remains the same; to protect the confidentiality, integrity, and availability of information assets. Furthermore, the most fundamental way of doing this is to ensure that only those who have a specific need for an asset, combined with specific authoritative permission, will be able to access that asset. That, in a nutshell, is access control.

TOPICS

Control access by applying the following concepts, methodologies, and techniques:

- Policies
- Types of controls: preventive, detective, corrective, etc.
- Techniques, e.g., nondiscretionary, discretionary, and mandatory
- Identification and authentication
- Decentralized and distributed access control techniques
- Authorization mechanisms
- Logging and monitoring
- Understand access control attacks
- Assess effectiveness of access controls
- Identity and access provisioning lifecycle

OBJECTIVES

According to the (ISC)^2 Candidate Information Bulletin, an information security professional should fully understand:

- Access control concepts, methodologies, and implementation within centralized and decentralized environments across the enterprise's computer systems.
- Access control techniques and detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

Key Access Control Concepts

Before beginning a comprehensive overview of the access control domain, it is important to have an understanding of some key concepts that will be important throughout the chapter. These concepts form the basis for understanding how access control works, why it is a key security discipline, and how each individual component to be discussed in this chapter relates to the overall access control universe.

The most fundamental and significant concept to master is a precise definition of what is meant by the term "access control." For the rest of this chapter and throughout this book, the following definition is used:

> ***Access Control*** is the process of allowing only authorized users, programs, or other computer systems (i.e. networks) to observe, modify, or otherwise take possession of the resources of a computer system. It is also a mechanism for limiting the use of some resources to authorized users.

In summary, access controls are the collection of mechanisms, processes or techniques that work together to protect the assets of an organization. They help protect against threats and mitigate vulnerabilities by reducing exposure to unauthorized activities and providing access to information and systems to only authorized people, processes or systems.

Although access control 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.

Additionally, almost all physical and logical entry points to the organization and its information systems need some type of access control. Given the pervasive nature and importance of access controls throughout the practice of security, it is necessary to understand the four key attributes of access control that enable good security management. Specifically, access controls enable management to:

- Specify which users can access a system or facility
- Specify what resources those users can access
- Specify what operations those users can perform
- Enforce accountability and non for those users' actions

Each of these four areas, although interrelated, represents an established and individual approach to defining an effective access control strategy. The information in this chapter will assist the security professional in determining the proper course of action to satisfy each of the attributes as it applies to a particular system, process, or facility.

Joining the C-I-A

The common thread among information security objectives is that they address at least one (if not all three) of the core security principles:

confidentiality, integrity, and availability (more commonly referred to as the C-I-A).

- ***Confidentiality*** refers to efforts made to prevent unauthorized disclosure of information to those who do not have the need, or right, to see it.
- ***Integrity*** refers to efforts made to prevent unauthorized or improper modification of systems and information. It also refers to the amount of trust that can be placed in a system and the accuracy of information within that system. For example, many systems and applications will check data that come into the system for syntactic and semantic accuracy to ensure that incoming data do not introduce operational or processing errors, thus affecting its overall integrity.
- ***Availability*** refers to efforts made to prevent disruption of service and productivity.

The goals of information security are to ensure the continued C-I-A 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.

The act of controlling access inherently provides features and benefits that protect the integrity of business assets. By preventing unauthorized or inappropriate access, organizations can achieve greater confidence in

data and system integrity. Without controls to manage who has access to specific resources, and what actions they are permitted to perform, there are a few alternate controls to ensure that information and systems are not modified by unwanted influences. Access controls (more specifically, records of access activity) also offer greater visibility into determining who or what may have altered data or system information, potentially affecting the integrity of those assets. Access controls can be used to match an entity (such as a person or a computer system) with the actions that entity takes against valuable assets, allowing organizations to have a better understanding of the state of their security posture.

Finally, access control processes go hand in hand with efforts to ensure the availability of resources within an organization. One of the most basic rules to embrace for any valuable asset, especially an asset whose criticality requires that it must be available for use over elongated periods of time, is that only people with a need to use that particular asset should be allowed access to that asset. Taking this stance ensures that the resource is not blocked or congested by people who have no business using it. This is why most organizations only allow their employees and other trusted individuals into their facilities or onto their corporate networks. In addition, restricting access to only those who need to use a resource reduces the likelihood that malicious agents can gain access and cause damage to the asset or that non-malicious individuals with unnecessary access can cause accidental damage.

Determining a Default Stance

An organization's access control strategy is directly influenced by its overall approach and philosophy concerning information security. For example, educational institutions and public social organizations generally promote more open and unfettered access to systems and information. They would most likely have fewer restrictions and controls on what information and services users can access. Their philosophy is based on allowing access to any information unless there is a specific need to restrict

that access. Such an access philosophy is often referred to as ***allow-by-default***. More formally, this philosophy dictates that any access that is not specifically denied is permitted. Even though such an organization may have security measures in place (like firewalls, for example), those devices are configured to allow access to a resource unless a specific resource is defined as requiring more restricted access. This approach provides a much more open environment for sharing information and resources, but at the potential cost of losing control over the confidentiality, integrity, and availability of the information and resources that organization manages. *Figure 1.1* shows a conceptual view of an allow-by-default environment.

In this illustration, the firewall is configured to allow most network protocols (e.g. FTP, HTTP, and SMTP) through to the organization's intranet. However, peer to peer (P2P) protocols (such as file sharing and instant messaging programs) are blocked at the firewall, presumably because the organization has determined they pose an unacceptable risk vs. the benefit they offer.

Other organizations have a much stricter access control philosophy. These include most commercial enterprises, government systems, and military installations. Their philosophy is one of ***deny-by-default***, or, more

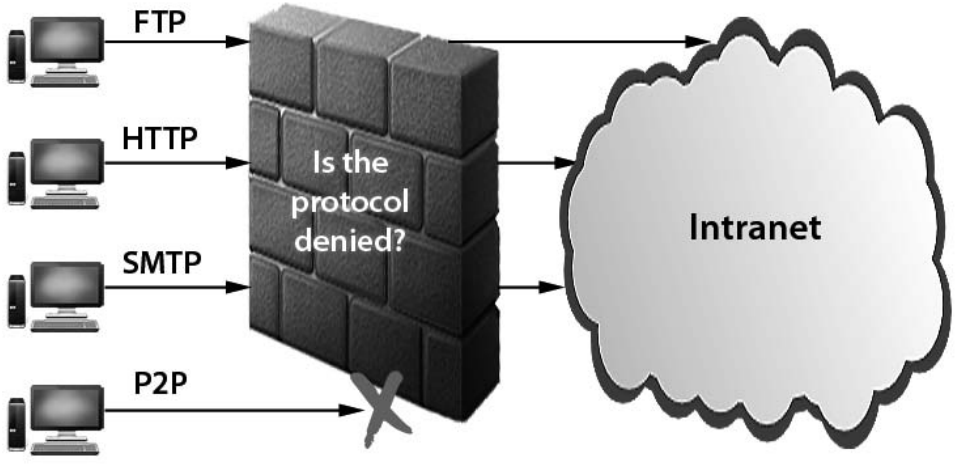


Figure 1.1 - **Conceptual view of an allow by default network environment**

formally, any access that is not specifically permitted is denied. In contrast to the allow-by-default approach, deny-by-default will block all attempts to access information and resources unless that access is specifically permitted. This approach provides an environment that protects information resources much more strongly, but at a cost of requiring much greater management and administration of those resources. In addition, workers in a deny-by-default environment may find that access to, and sharing of, information in such an environment is much more difficult. *Figure 1.2* shows a conceptual view of an allow-by-default environment.

In this diagram, the more restrictive environment blocks most protocols from entering the intranet. The exception is the SMTP protocol (used by most e-mail systems), which is allowed to pass through the firewall. This would allow e-mail traffic to travel in and out of the organization. In practice, few organizations follow pure allow-by-default or deny by default practices. Some areas of an organization may be more permissive (e.g., employee recreational information or cafeteria meal schedules), while other areas such as employee health and salary information or company financial records may be much more restrictive. Nevertheless, most organizations will have one or the other of these core philosophies as their underlying guiding principle for access control. Defining a core philosophy is very

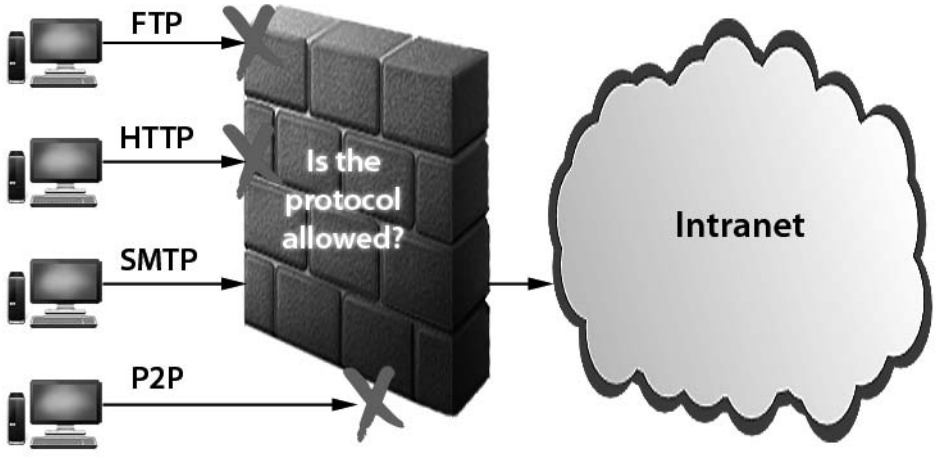


Figure 1.2 - **Conceptual view of an deny by default network environment**

important for a successful access control strategy, as it sets the tone for all other access control decisions to follow.

Defense in Depth

The practice of implementing appropriate access control mechanisms is also the first line of defense in an organization's ***defense-in-depth*** strategy. Defense in depth is the practice of applying multiple layers of security protection between an information resource and a potential attacker. If one of those layers should fail the successive layers will continue to function and protect the resource against compromise. A sound access control strategy provides the first layer of protection. By carefully managing all attempts to access a resource and blocking those that are not preauthorized, it ensures that all the other layers protecting that resource have a much greater chance of successfully protecting it. Defense in depth is applicable to both the physical and virtual environments. For example, imagine a modern office complex where top-secret data are stored, as depicted in *Figure 1.3*. In such an environment, a tall perimeter fence might provide the first layer of defense to keep intruders out. If an intruder gets through the fence, the building may have an armed guard at the front door. Should the intruder manage to knock out and disarm the guard, he may find that the building requires an access card to get past the main lobby. If the intruder can find an access card (perhaps from the security guard he just knocked out), and get into the main part of the building, he may find that all the cabinets with secret data are locked and the key is nowhere to be found! The goal in all of this is to ensure that access to target assets (in this case the secret data) is protected by multiple layers of controls.

A properly protected virtual environment, such as that depicted in *Figure 1.4*, should present similar challenges. If that same intruder decided to break into the company's data center over the Internet he may find that the company's network is protected by a strong firewall. However, this intrepid villain does not let that stop him and manages to find a hole through the firewall to the company's payroll server. The server, however,

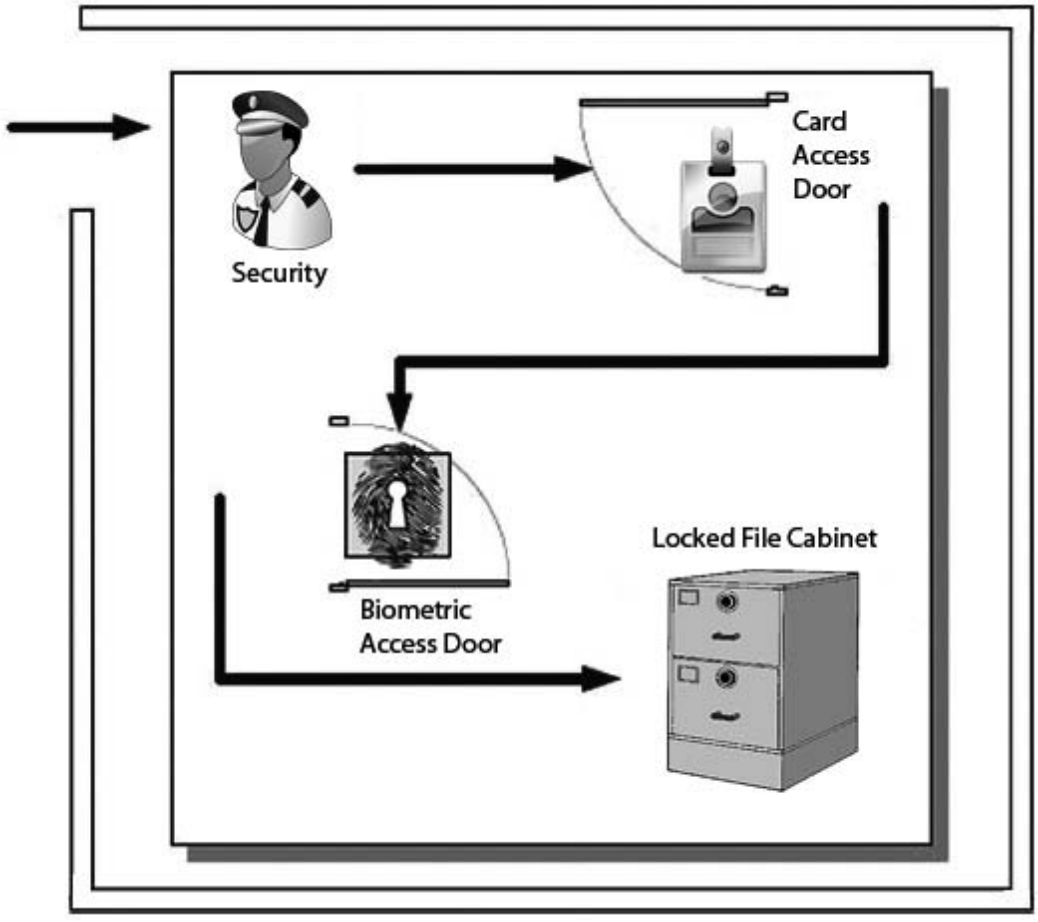


Figure 1.3 - **Physical defense in depth**

requires a password. If the attacker keeps going he will find that the applications on the server also require passwords, the system is protected by a host-based Intrusion Prevention System (more on that later), and the database files are encrypted. As it was with the physical security example, the more layers of protection placed between an attacker and a potential target the less likely it is that the failure of any single control will cause compromise or loss of the asset. Access controls can be found in many places within a computing environment. For example, firewalls employ rules that permit, limit, or deny access to various network services. By reducing the exposure to threats, controls protect potentially vulnerable system services, ensuring that network's availability. By reducing exposure to unwanted and unauthorized entities, organizations can limit the

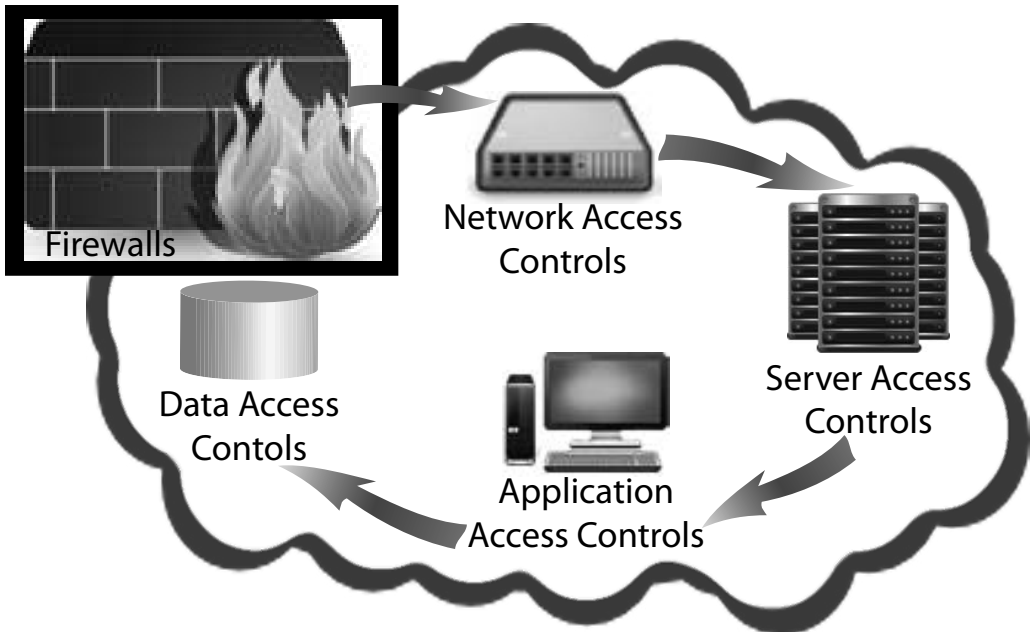


Figure 1.4 - **Network defense in depth**

number of threats that can affect the availability of systems, services, and data.

Access Control: A General Process

There are many different approaches to implementing an access control scheme—almost as many as there are security professionals. However, there is a general approach that is applicable to almost any situation and provides a useful framework for determining access controls. The three-step process is:

1. Defining resources
2. Determining users
3. Specifying the users' use of the resources

Step 1: Defining Resources

The first step to enable an effective access control strategy is to specifically define the resources that exist in the environment for users to access. Essentially, this step answers the fundamental security question, "What

are you trying to protect?" While this may seem intuitive, this is not a step that should be overlooked, nor should its importance or potential complexity be underestimated. The definition of what exactly constitutes a "resource" to an organization may take considerable discussion, but once it is decided it will clarify and simplify the process of identifying those resources that are important enough for the organization to protect.

The proper definition of the available resources in your organization must also be coupled with a determination as to how each of those resources may be accessed. Do users need a specific organizational status to access a particular resource, or is it enough just to be a member of a specific project? Accessing information on a company's benefit plans may simply require a person to be an employee, whereas accessing quarterly financial projects may specifically require a person to be part of the finance organization. Addressing these issues during this step will also lay the foundation for effectively implementing role-based or domain-based access controls, which will be discussed later in this chapter.

It is also essential to bind a user, group, or entity to the resources each is accessing. Resources can include data, applications, services, servers, storage, processes, printers, or anything that represents an asset to the organization that can be utilized by a user. Every resource, no matter how mundane, is an asset that must be afforded protection from unwanted influences and unauthorized use. This includes important resources like internally developed software, manufacturing systems, employee personnel files, or secret product formulas. However, it may also include often-overlooked resources like printers, fax machines, and even office supplies. The actual amount of protection to give each resource may be based on a cost–benefit analysis of the effort required to provide the protection or it may be based on a particular risk or threat model favored by the organization. Once the required resources are determined, then controls can be defined to specify the level of access.

Step 2: Determining Users

The next step in managing access control is defining who can access a given resource. The concept of identifying who are permitted access and providing the credentials necessary for their role is fundamental to security and ancient in practice. In early tribal cultures, a rite of passage consisted of obtaining a specific garment, marking, or even a scar signifying you were approved for various activities within the tribe, which translated to access. As populations grew and became more sophisticated, new methods were developed to provide access to an approved community. Over 4000 years ago, the Egyptians developed the first lock-and-key systems. Wooden locks were operated by a wooden key that controlled pins to disengage a bolt and permit access to the protected object. The key would be provided only to those who had been identified as needing access. Although seemingly primitive by today's standards (after all, how long would a wooden lock protect a modern file cabinet?), the technology and social conventions of the day allowed this to be quite an effective mechanism in ancient Egypt. Today security professionals continue the tradition of using the latest in available technology to protect valuable assets.

A typical environment must manage employees, contractors, consultants, partners, clients, or even, on occasion, competitors that organizations need to identify as requiring access of one kind or another. The act of specifying which users can have access to a system is typically driven by an operational demand, such as providing access to an accounting system so that users in the financial department can record and pay bills. Access control decisions are often based on organizational, social, or political considerations as well. One's personal or functional status within the organization may dictate the type or scope of access to organizational assets that may be allotted. A company CEO is rarely denied access to any organizational asset he may request; despite the fact that his explicit need to have that information may not be readily apparent. While this may not be the preferable method of determining access rights, a real-world information security manager should be prepared to deal with such situations.

The most significant aspect of determining which users will be provided access is a clear understanding of the needs of the user and the level of trust given to that person or entity. An identification process must exist that takes into consideration the validity of the access need in the light of business needs, organizational policy, legal requirements, information sensitivity, and security risk. It is important to understand that with each new user or community, the threat profile of an organization changes. For example, an organization may determine that one of its partners needs access to a given system. Upon providing that access, the potential threats to the organization now include that partner organization. Not only must the relationship be founded on trust, established by legal or other mechanisms between the two entities, but it must also now consider the increase in the number of users, thereby increasing the potential sources of threat. The more sophisticated the access control system, the greater the number of options to support various access demands in a secure fashion. It is not uncommon for organizations to have several different access control strategies to accommodate various needs, resulting in the provisioning of multiple unique access solutions. However, this is not considered as a security best practice, and the objective is to have a consistent access control strategy to avoid too much complexity. The more the complexity that exists in any system, including access control systems, the more likely it is that unexpected interactions will cause security flaws to be exposed. Simplicity is the key to any effective security system. The overall goal, then, is to strike an effective balance between the need to manage the complex access needs of an organization and the need to keep the access control system as simple as possible to understand and manage.

Step 3: Specifying Use

The final step in the access control process is to specify the level of use for a given resource and the permitted user actions on that resource. Take, for example, the files and data resident on a typical computer. Most file systems provide multiple levels of permissions, such as read, write, and execute. Depending on the file system used to store data, there may be

methods of permitting much more granular controls. These may include the ability to provide access to a specific user, but only permitting him or her to perform a certain task. For example, a user with the role of "data backup" will be allowed to perform administrative functions such as "copy to tape," but not to erase or alter the information. (Access permissions will be covered in greater detail later in this chapter.) Additionally, a user may have the need to run an application, and therefore be provided execute privileges. However, he may not have write privileges, to ensure that he cannot modify the application. The same philosophy can be applied to any resource, and access controls should be used to support an organization's business functionality. For example, to restrict a user's ability to access specific printers based on a particular organizational structure. This would, as an example, allow a department to restrict high-cost color printing to only the members of the graphics or marketing departments. Not only would this properly restrict access to valuable and expensive resources, it might also aid the organization's cost allocation efforts by ensuring that charges for those resources are allocated only to those who must use them. As another example, an organization that needs to restrict printing and duplication of sensitive or classified documents may allow any user to send a print job to a particular printer, but require another level of approval from an authorized official to actually print the document in order to avoid policy violations.

Ultimately, once a user is identified and authenticated, an access control system must be sensitive to the level of authorization for that user to use the identified resources. Therefore, it is not enough to simply identify and authenticate a user in order to access resources. It is also necessary to control what actions are permitted for a specified resource based on the user's role (unless, of course, "unlimited access" is the organizational policy).

Access Control Principles

Access Control Policy

The first element of an effective access control program is to establish an access control policy and associated standards and procedures. An access control policy specifies the guidelines for how users are identified and authenticated and the level of access granted to resources. The existence of an access control policy ensures that decisions governing the access to enterprise assets are based on a formalized organizational directive. The absence of a policy will result in inconsistencies in provisioning, management, and administration of access controls. The policy will provide the framework for the definition of necessary procedures, guidelines, standards, and best practices concerning the oversight of access management.

Separation of Duties

It is often possible to enable effective access controls by altering the way people perform their work functions. The primary objective of separation of duties is the prevention of fraud and errors. This objective is achieved by distributing the tasks and associated privileges for a specific process among multiple people. It acts as a deterrent to fraud or concealment because collusion with another individual is required to complete a fraudulent act, ensuring that no individual acting alone can compromise the security of a system or gain unauthorized access to data. Of course, just because separation of duties is established for a given process does not mean that fraud is impossible to carry out; it just means that it is more difficult. People are generally averse to include others in the planning of criminal acts, so forcing collusion to happen in order to carry out such an act reduces the overall risk of its occurrence.

The first action to employ separation of duties in a process or work function is defining the individual elements of that process. Processes are typically a collection of tasks that must be performed to achieve an objective. Examples of common processes include performing backups, copying

files, or granting system access. Work functions can also encompass highly complex and potentially vital (or dangerous) business elements that should not be in the control of any one person. A common example is the process of creating and approving requisitions for purchasing expensive items. The person who requests the expenditure should not also be allowed to approve the expenditure. This prevents a single person from creating and receiving fraudulent payments. A less common, though more dangerous, example from the military is the ability to launch nuclear missiles. One person may have the ability to arm the missile but not execute the launch sequence. Another person may have the ability to launch the missile but not arm its payload. Finally, neither person can do anything without receiving proper authorization from the President. In this case, all three people are needed in order to successfully launch an armed missile. This safeguard ensures that a single person with a political agenda (or just having a particularly bad day) will not be able to start a global nuclear war.

To determine the applicability of separation of duties, two distinct factors must be addressed: the sensitivity of the function under consideration and the elements within a process that lend themselves to distribution. Sensitivity of the function takes into consideration the criticality of the job performed and potential exposure to fraud, misuse, or negligence. It will be necessary to evaluate the importance of a given transaction and its relationship to enterprise security risk, operations, and, of course, C-I-A factors. It is important to be aware that seemingly mundane tasks may also sometimes require separation of duties practices. For example, a single user performing both backup and restore procedures would have the ability to manipulate or destroy the backup data to cover unauthorized activity, change information, or destroy valuable resources undetected.

There are other activities within an organization that are not only important when considering separation of duties, but their technical and procedural architecture also assists in establishing these controls as well. For example, in application development there are typically separate

development, testing, and production environments. The integrity of libraries used for the development is critical, and it is important that live systems and proprietary information should not be used within the testing environment to mitigate the risk of exposing sensitive information. Therefore, the development environment needs to follow strict separation of duties throughout the process in order to ensure that code and data follow strict change management processes and access by personnel between these areas is restricted. This reduces the risk of changes being made to the code once it has been tested and ensures the integrity of the tested code and that the production code is maintained.

The second factor when determining the applicability of separation of duties is understanding what elements within a function are prone to abuse, which ones are easily segmented without significantly disrupting operations, and what skills are available to the pool of users performing the different elements of the function. These can be summarized as

1. Element identification, importance, and criticality
2. Operational considerations
3. User skills and availability

Element Identification, Importance, and Criticality

Each function will have one or more elements that must be performed to complete the transaction. Some elements within a function, known as milestone elements, may lend themselves to offer opportunities for fraud or abuse. Such cases would then require a different user with unique privileges to complete that element. To ensure that a process runs as efficiently as possible within a separation of duties environment, it may be possible to collect different elements into groups that together represent a milestone element. The key is to evaluate each element and the role it plays in performing the function. Once each element is assessed against the potential for abuse, they can begin to be distributed to various users.

In the event that a collection of elements within a function does not

offer a clear point of segmentation, it may be necessary to incorporate a new milestone element as a validation and approval point within the function. For example, at a specific point in a process, a manager can send an e-mail, apply a digital signature, or add a validation mark to the data. That additional notification or mark must be present for the primary user to continue the remaining processes.

Operational Considerations

One of the key attributes of a successful security program is integrating effectively within the business or operational goals of the organization. When considering separation of duties, the impact to the function and its role in the business are essential to overall success. When implemented poorly, or without taking overall business goals into account, security-related processes like separation of duties can hinder the process and make it prone to circumvention.

The impact to the operations must be taken into account whenever establishing separation of duties practices for a function. The security manager must consider the impact to the efficient operation of the function as well as the meaningful alternative options in the event there is a system failure or outage. It is important not to sacrifice security, but rather to have alternate compensating controls that can meet the objectives for security.

In addition, the cost of implementing separation of duties within a business process must be weighed against the overall risk that process represents to the organization and whether the benefits of separation outweigh the time and effort costs to the organization. In the separation of duties example of arming and launching nuclear missiles, it can be nearly universally agreed that the cost of implementing separation in such a circumstance is greatly outweighed by the risk and potential harm that could come from a non-separated nuclear environment. Conversely, most would agree that implementing separation of duties in a cafeteria's tuna sandwich-making process would not make a great deal of sense. While it is true that a malevolent sandwich maker could intentionally inflict illness

or even death upon unsuspecting patrons, the actual incidence of such an occurrence is relatively low and the addition of the extra personnel required for such a low-risk situation would be very costly to the organization.

User Skills and Availability

Clearly, separation of duties requires multiple participants, and each of those participants must have the appropriate skills and training to perform the specific element of a given function. Additionally, there must be enough personnel to perform all the elements that have been distributed. In organizations that have small staffs, pure separation of duties may not be feasible. For example, a common separation practice is to ensure that those who develop software programs should not have access to the production environments where those programs are run. Those who run and maintain the production environment should be a separate and distinct group from the development team. This separation prevents a rogue developer from introducing malicious code directly into a production system. Unfortunately, many small development shops and start-up companies cannot afford the extra personnel that such a separation environment requires. Staffing those extra positions may just mean the difference between a successful business and bankruptcy. Given the tradeoff between the benefits of separation (prevention against malicious code) and the cost of separation (double the salary expense), a reasonable business owner might opt against separation, preferring instead to instill other mitigating controls to reduce the risk, such as a strong change management process and code reviews.

The following concepts are important in ensuring appropriate application in policy and practice:

> ***Least Privilege:*** The principle of least privilege is one of the most fundamental characteristics of access control for meeting security objectives. Least privilege requires that a user or process be given no more access privilege than necessary to perform a job, task, or function. The objective is to limit users and processes to access only

resources and tools necessary to perform assigned functions. This often requires limits not only on what resources can be accessed, but also includes limiting the actions that can be performed by the user even if they have authorized access to the resource. For example, a user may be restricted to only read-only, update, and execute permission on a system without the ability to create or delete files and databases. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges required to perform that job, and restricting the user to a domain with those privileges and nothing more. Denying users access privileges that are not necessary for the performance of their duties ensures that those privileges cannot be used to circumvent the organization's security policy.

Need to Know: A companion concept to least privilege is the notion of need to know. If the goal of least privilege is to reduce access to a bare minimum, need to know defines that minimum as a need for that access based on job or business requirements. For example, although the CIO in an organization has the appropriate rank in the organization to view upcoming quarterly financial forecasts, the organization's comptroller may decide that the CIO does not have a need to know that information and, thus, restrict access to it. Need to know is also used heavily in situations where operational secrecy is a key concern, such as in military operations. Military leaders often keep operational plans on a need to know basis to reduce the number of people who know about the plans and reduce the risk that someone will leak that information to the enemy.

Compartmentalization: Finally, compartmentalization completes the least privilege picture. Compartmentalization is the process of separating groups of people and information such that each group is isolated from the others and information does not flow between groups. For example, an organization might compartmentalize (both logically and physically) a team working on mergers and

acquisitions so that the information that team is working on will not leak to the general employee population and lead to a potential insider trading problem. Compartmentalization is helpful in situations where information needs to stay contained within a single group or area and strong protections need to be taken to keep that information from leaking outside the area.

Security Domain: A security domain is an area where common processes and security controls work to separate all entities involved in these processes from other entities or security domains. For example, all systems and users managing financial information might be separated into their own security domain, and all systems involved in e-commerce activity might get their own security domain. A security domain is based on trust between resources or services in areas or systems that share a single security policy and a single management structure. The trust is the unique context in which a program is operating. There may be multiple security domains within an organization and an entity may, at times, belong to more than one security domain based on its responsibilities and functions at any given time. The separation between domains can be either physically or logically managed. Security domains support a hierarchical relationship where subjects can access objects in equal or lower domains; therefore, domains with higher privileges are protected from domains with lesser privileges.

In *Figure 1.5*, three distinct and separate security domains exist on the server, and only those individuals or subjects authorized can have access to the information on a particular domain.

A subject's domain, which contains all of the objects that the subject can access, is kept isolated. Shared objects may have more than one access by subjects, and this allows this concept to work. For example, if a hundred subjects have access to the same object, that object has to appear in a hundred different domains to allow this isolation.

Information Classification

Many organizations have thousands, even millions, of data files containing valuable information on all aspects of the organization's business. Information is created in great volumes on a daily basis from a variety of transactional systems, as well as aggregated into databases and data warehouses to provide decision-making support. The information is stored on backup tapes, copied to portable USB drives, and burned to CDs and DVDs for portability. Information is stored on portable computers and network drives, and in e-mail systems to support the sharing of information.

The same information is printed and filed, and stored off site for business continuity and disaster recovery purposes. A file will typically have multiple versions, will be stored in multiple locations, and is capable of being accessed by different individuals in each of these locations. Fundamental security questions are raised in this type of environment. Where is the organization's information? How should the information be handled and protected? Who should have access to it? Who owns the information? Who makes the decisions around these parameters? These questions form the impetus for implementing an information classification strategy. Information classification is the practice of evaluating the risk level of the organization's information to ensure that the information receives the appropriate level of protection. The application of security controls to information has a cost of time, people, hardware, software, and ongoing maintenance resources that must be considered.

Applying the same level of control to all of the company's assets wastes resources and money by overprotecting some information and underprotecting other information. In an effort to simplify security budget management, security dollars are often spent uniformly to protect all assets at the same level. Not all assets have the same value or need the same level of protection. The budget could be better allocated, and the security of the organization better managed, by providing only basic protection to assets of little value and providing increased protection to those assets considered

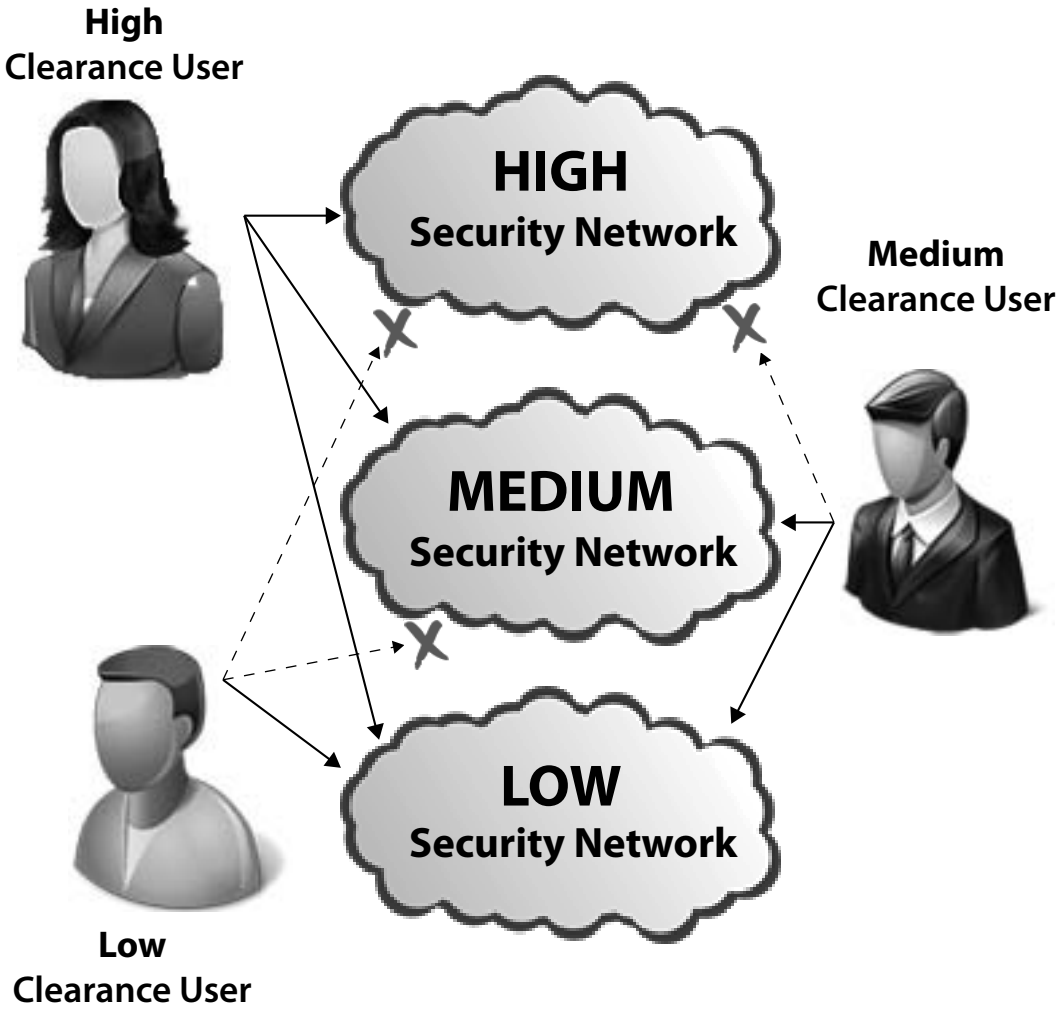


Figure 1.5 **- Three distinct and separate security domains exist on the server. Only those individuals or subjects authorized can have access to the information on a particular domain.**

to be of greater value or higher sensitivity. By applying protection controls to the information based upon the classification, the organization gains efficiencies and thus reduces the overall cost of information security. The primary objective of information classification, therefore, is to group an organization's information assets by levels of sensitivity and criticality. Once this is done, the organization then applies the appropriate level of protection controls to each asset in accordance with the classification assigned to it.

Information Classification Benefits

There are many benefits in classifying information within an organization. First, classification helps to establish ownership of the information, which provides a central point of control for all aspects of security and access to the information. This increases the likelihood that the information will be used in the proper context and those accessing the information will be properly authorized. Information classification also increases the confidentiality, integrity, and availability of information by focusing an organization's limited security funds on the resources requiring the highest level of protection and providing lesser controls for the information with less risk of loss. By understanding the information and its location, the organization can identify areas that may need higher levels of protection. Information classification can also have a positive effect on the knowledge and awareness of security within an organization. A classification program allows for greater understanding of the value of the information to be protected, and provides a clearer direction for the handling of sensitive information. In addition, a periodic review of the classification scheme and controls helps personnel maintain awareness of the importance of protecting information. Finally, the process itself helps create a greater organizational awareness of the need to protect company information.

Information classification can also have an operational benefit to the organization. Critical information can be identified to support business recovery scenarios by focusing the recovery efforts on the most critical areas. Placement of information with higher levels of classification on more reliable storage and backup mechanisms helps reduce recovery times. Organizations can also reduce the expense of inefficient storage for non-sensitive information in data storage or physical file cabinets through the use of a well-planned information classification program.

Establishing an Information Classification Program

Establishing an information classification strategy and developing plans for implementation may seem a bit onerous for an organization that has

never had such a program before. However, once the work of defining the classification levels and determining the classification of the individual information has been completed, the value to the organization is well worth the effort. The following sections walk through the steps of establishing and sustaining an information classification program. Although the exact path each organization takes may be a bit different, the steps identified are a good representation of the major steps involved in programs of this type. The exact sequence or the steps included may also vary or be combined, depending upon the size, complexity, and culture of the organization. The basic steps are

1. Determine inforation classification program objectives.
2. Establish organizational support.
3. Develop an information classification policy and supporting procedures.
4. Develop information classification process flows and procedures.
5. Develop tools to support the process.
6. Identify process or application owners.
7. Identify information owners and delegates.
8. Distribute standard templates.
9. Classify information and applications.
10. Develop auditing procedures.
11. Load classification information into a central repository.
12. Train users.
13. Periodically review and update information classifications.

Step 1: Determine Information Classification Program Objectives

It is helpful to document the specific program objectives to give the program a clear vision of its goals and to help define and explain the program to others in the organization. Defining clear objectives also helps to contain the scope of the effort and determine when deliverables are completed, so

that these accomplishments may be celebrated to sustain those involved in later phases of the project. The objectives are also important for obtaining the support of those needed to both endorse and carry out the program.

It is very important when defining the overall program objectives to clearly establish that information classification is a program, not a project. A project is a series of tasks that lead to a known end state. A program, on the other hand, is a change in organization process and behavior that will have long-term lasting impact to the organization. Implementing information classification in an organization will change the way the organization thinks about and manages information permanently and, thus, has no defined end state to speak of. It is truly a program in all meaningful respects and should always be referred to as such.

Step 2: Establish Organizational Support

Senior management support is essential to the start-up and continued operation of the information classification program. The program should be socialized with senior management by using business-focused benefits, as well as highlighting enhancements to the effectiveness of the organization. There may be a perception within the organization that all information should be treated as confidential and is adequately secured by physical barriers to the facility, firewalls, and other security controls protecting the environment. This view promotes the concept that all information should be protected equally. Unfortunately, the reality is that information resources should be given the appropriate protection based on their overall risk and threat profile: no more and no less. The security professional should work through the cost/benefit discussion with senior management to illustrate how the appropriate application of security controls is the most effective approach to benefit the business. Although security professionals understand the importance of information classification, without the proper positioning of the effort, the organization's senior management and end users may perceive the effort as another project requiring their resources, with little payback to individual departments. Some examples

of the benefits that the organization may realize as a result of these efforts include:

- Ensuring confidentiality of information by restricting who can access or copy the information
- Increased accuracy and integrity of information by controlling who can modify or update the information
- Increased availability of information by restricting the ability to overwrite or erase important or critical data
- Avoiding damage to the organization's reputation by reducing the risk of unauthorized disclosures
- Reduction in costs of overprotection
- Ability for managers to enforce accountability
- Protection of intellectual property and trade secrets
- Protection of customer or consumer confidential information
- Compliance with industry regulation or legal requirements to protect personally identifiable information

Step 3: Develop an Information Classification Policy and Supporting Procedures

The information classification policy communicates the requirement to the organization to classify the information assets. The policy also communicates the primary purpose of information classification, which is to ensure that the appropriate protections are applied according to the level of sensitivity, risk, and criticality. The policy statement is a description of the requirement, including the scope of users and systems to which the policy applies, as well as what is expected of those affected by the program. The policy should describe the overall information classification framework and the meaning of each level or categorization within the framework.

The policy may also indicate the responsibilities of users and management in handling the information. Policies are generally written

at a high level, with the details reserved for supporting procedures. The procedures communicate how to determine the classification of a particular information item, as well as how that information should be subsequently handled and protected. Involvement with business or application owners, as well as the IT department, is important in determining the various procedure and control matrices. This establishes business owners' buy-in to the procedures, and provides an operational perspective for determining how the information should be managed.

Step 4: Develop Information Classification Process Flow and Procedures

Documented procedures assist in the ongoing operation of classifying information. Because the organization may have many files that have not been looked at through the information classification lens, the start-up effort to develop these flows and procedures may require a large amount of resources. Ongoing efforts will also require that the information is reviewed and updated on a periodic basis. The initial gathering of the information classifications and the process utilized must be driven by a documented procedure so that all of the parties involved in the effort are aware of their individual roles and requirements to complete the classification. Flowcharts in addition to the documented written processes can be helpful, as individuals receive and retain information through different means. The documentation of the process also helps ensure that the classification process is handled uniformly throughout the organization.

Step 5: Develop or Acquire Tools to Support Process

Various tools, such as word processing documents, spreadsheets, databases, and presentations, support the collection process. Standardized templates facilitate collection as well as the ability to generate reports by data type to ensure that the designations are consistent across the enterprise and follow the prescribed information classification policy and associated standards. Once the chosen media and forms are distributed to the individuals completing the information, the results can be exported to a database for consolidation, review, and ongoing maintenance.

Step 6: Identify Process or Application Owners

The business owner of each application provides the functional requirements for what data is necessary for the business. The owner will have the most intimate knowledge of the data and how they are used. Apart from the business owner, the systems or information technology owner may act primarily as a data custodian of the information and must understand the processing, technical, storage, and security protections of the information. Both individuals contribute to an understanding of the classification requirements and is identified as part of the process. The relationship between the information owner, system owner and application owner will greatly influence the ability to make changes and identify stakeholders. When an information system owner and information owner are one and the same they generally have a greater motivation to make system security enhances which protect the information they must protect.

Step 7: Identify Information Owners and Delegates

Information owners are those people in the organization who understand the information in their area of the business and have the ultimate responsibility for making decisions about the usage of the information. They may manage the responsibility or assign designees or information delegates that are empowered to make the day-to-day operational decisions as to who is allowed to read, modify, or delete the business information. The owners and delegates are the primary individuals who are involved in the classification process, as they have the greatest business knowledge of the information in question.

Step 8: Distribute Standard Templates

Providing standard information classification templates to data owners promotes uniform data gathering and makes the subsequent tasks of tracking and analysis of the information much easier. The templates may be part of the tools developed in Step 5. These templates should be distributed to the information owners or delegates to collect the classification information on the data managed by their departments.

Step 9: Classify Information and Applications

Once the templates have been distributed, the data owners (or their delegates) use the information classification policy and standards to classify the information. Typically there are three to four levels of information classification used by most organizations:

- ***Public:*** Information that may be disclosed to the general public without concern for harming the company, employees, or business partners. No special protections are required, and information in this category is sometimes referred to as unclassified. For example, information that is posted to a company's public Internet site, publicly released announcements, marketing materials, cafeteria menus, and any internal documents that would not present harm to the company if they were disclosed would be classified as public. While there is little concern for confidentiality, integrity and availability should be considered.
- ***Internal Use Only:*** Information that could be disclosed within the company, but could harm the company if disclosed externally. Information such as customer lists, vendor pricing, organizational policies, standards and procedures, and internal organization announcements would need baseline security protections, but do not rise to the level of protection as confidential information. In other words, the information may be used freely within the company but any unapproved use outside the company can pose a chance of harm.
- ***Confidential:*** Information that, if released or disclosed outside of the organization, would create severe problems for the organization. For example, information that provides a competitive advantage is important to the technical or financial success (like trade secrets, intellectual property, or research designs), or protects the privacy of individuals would be considered confidential. Information may include payroll information, health records, credit information, formulas, technical designs, restricted regulatory information, senior

management internal correspondence, or business strategies or plans. These may also be called top secret, privileged, personal, sensitive, or highly confidential. In other words this information is ok within a defined group in the company such as marketing or sales, but is not suited for release to anyone else in the company without permission.

- ***Restricted:*** Information that requires the utmost protection or, if discovered by unauthorized personnel, would cause irreparable harm to the organization would have the highest level of classification. There may be very few pieces of information like this within an organization, but data classified at this level requires all the access control and protection mechanisms available to the organization. Even when information classified at this level exists, there will be few copies of it around, and tracking who has this information, when they received it, and when they returned it are extremely important. Information of this type includes merger and acquisition information, financial forecasts, or anything that (if publicly known) would materially affect the market status or stock price of the company. In other works information of this type is typically only suitable for a select few individuals such as "C" level executives and cause grave damage to the company if released outside of this group.

An important point to consider is that this process may take a long time to complete, especially if you are analyzing and classifying a large environment with complex data relationships. When faced with such a seemingly daunting task, data owners will often react by arguing against the process based on the cost of the analysis alone or relegating the project to back-burner status where it will receive little, if any, attention. It is important to work with all the data owners and senior management to ensure that the program remains on track. There are some steps you can take to reduce the amount of time required for the initial classification effort. For example, a data owner may have a database with thousands of intermingled data elements fitting into all three classification levels. Rather

than classifying each individual data element and applying appropriate controls at the element level, the owner may elect to reorganize the database into public and nonpublic data sets and apply the appropriate controls in aggregate to each data set. While the process of such aggregation may lead to the oversimplification problem mentioned earlier, if applied judiciously it can lead to enormous time savings during the classification process and cost savings during the implementation of protection controls.

During the planning and design of the classification program some consideration should be given to the classification of aggregate data. This is information that would not be considered sensitive when taken alone, but, when combined with other data, suddenly becomes sensitive and worthy of additional protection. For example, a bank routing number (the number found at the bottom of a check that uniquely identifies a U.S. financial institution) by itself would not be considered particularly sensitive by a data owner. Routing numbers are public information easily found through a simple Internet search. However, when that routing number is combined with an individual account number at that bank, the combination of the two suddenly becomes very sensitive, because a thief can use that combination to access that individual's bank account. Data owners need to be aware of the dangers of aggregate data and account for them during the classification of their information.

In many circumstances one organization will be managing information on behalf of another organization. For example, many companies outsource their payroll processing to third parties and many banks outsource their IT systems (including account management) to third-party service providers. In these cases, the company that owns the information and the service provider may each have its own classification systems. It is important that each party understand the other's classification system and the information owner must ensure that the classification assigned to its information by the service provider (as well as the underlying protection mechanisms for that classification) meets its needs for adequate information protection.

Step 10 Develop Auditing Procedures

Once information is classified, classifications rarely change unless the information has been misclassified, the information that previously required protection is now public knowledge, or time has made wider disclosure of the information less harmful to the organization. In most cases, if there was a reason to protect the information initially to a certain level, then the information will continue to be protected at this same level through its useful life. However, new data are always being generated and needs to be classified. Existing data should also be periodically reviewed to ensure that the classifications are correct. Information classification auditing is the process of reviewing the classifications to ensure the accuracy of the information, thus ensuring that the appropriate security protections continue to be applied. An information classification audit often relies on performing "spot" tests such as observations of sensitive information left unprotected in work spaces (also known as a clean desk/clear screen check) and checking of trash receptacles for discarded sensitive information as a method to measure compliance with the information classification policy.

Step 11: Load Clssification Information into a Central Repository.

The classification information obtained through the classification procedures and templates is loaded into a central repository to support the analysis of the collections, as well as to serve as the database for the ongoing updating of the classifications. A database tool provides the ability to examine the information from multiple perspectives, such as listing all of the data types owned by a particular data owner, all of the data types of a particular classification level, or what data types are associated with which applications. Depending on the amount of assets being classified and the complexity of the classification scheme, the database may grow to considerable size. Careful planning is important to ensure adequate space and processing capacity for the future.

Step 12: Train Users

If the end user or employee does not understand what information is public, internal user only, or confidential, or if the user does not

understand the requirements and differences in how to handle each type of information, then the investment in information classification will have limited success. It is critical that the user community gets proper training in the classification program because they (the users) are the ones who will work with the program on a daily basis. The training program must convey the purpose and importance of the program and provide the proper motivation for users to support the classification effort. Training should include information on the overall policies and the various classification levels the organization will use. Most importantly, the training should give practical examples of different types of information the users will come in contact with and how to properly handle and protect that information using the official standards and protection controls.

Step 13: Periodically Review

Periodically review and Update Information Classifications: Information within an organization rarely remains static. To ensure that the organization continues to match current threats with appropriate information protections, the classifications assigned to information must be reviewed on a periodic basis. It is most likely that the classifications will not change dramatically, but adjustments may be needed. Scheduling auditing procedures on a periodic basis increases the quality of the information classification program, as does providing the capability to update and add new information classifications outside of the normal cycle.

Labeling and Marking

The labeling and marking of media with classification levels provides the ability to manage the information contained within the media with the handling instructions appropriate to the respective classification. For example, a backup tape may be labeled with a serial number and "Company Confidential" to indicate how the information should be treated. Organizations may decide not to label individual information, but rather control all the information within a business area or location according to restrictions based upon a single classification type. For example, all

backup tapes in the tape library may be classified as "Confidential" and have appropriate controls placed on the whole library.

Labeling and marking information also apply to all forms of systems and media that manage or display classified information. This includes application displays, printouts, and reports generated from organization systems. All these must have the appropriate classification verbiage displayed or printed alongside the information to ensure that all who come in contact with that information know the classification level and are able to take the appropriate protective measures.

Information Classification Assurance

Periodically testing the information classifications provides assurance that the activities are being properly performed. The audit procedures will uncover those data types that need to be added or reclassified. Random audits of user areas, such as checking desktops for confidential documents not returned to file drawers, information left overnight in open shredding bins, files in electronic file folders accessible by anyone within the organization, confidential information posted to a public Web site, or information left on copiers, printers, and fax machines, can provide information regarding organizational compliance. Encouraging end users to report security incidents related to mishandling of classified information can also be a source to provide assurance. The information security manager should work closely with the organization's internal audit manager to establish information classification reviews as part of the standard audit program. In this way, the audit group can assist in ensuring the continual monitoring of the classification program including the assurance that new information is classified appropriately as it enters the environment.

Access Control Requirements

As simple as it may seem, implementing an effective access control system—whether for a single application or for an entire enterprise—takes careful planning, research, foresight, and (of course) a great deal of persuasive

skill to bring together all the disparate interests in the organization to agree on the best way to move forward. However, none of this can proceed without first considering the basic requirements that any access control system must meet. While each enterprise or application will have its own specific access control needs, there are some basic considerations that all security professionals must look for in an access control system, process, or technology. This section will discuss several of those requirements.

Reliability

First and foremost, any access control system under consideration must be reliable enough to give consistent results every time. The reliability of a system has both physical and logical components. Both are important to consider when determining the best path for an organization to take. An access control system must operate within the same physical environmental constraints under which its users operate. This means that all the environmental factors that assist or hinder its users will have the same effect on the access control system. Factors such as heat, humidity, complexity, wear and tear on components, and user attitude will all have an effect on the long-term viability of the environment. For example, if a badge reading system is used in a busy area (like a hospital emergency room or fire house) it will most likely be subject to physical abuse as users hurry to swipe their cards through the reader, perhaps knocking or banging it repeatedly in the process. It will get heavily abused as frustrated and busy users take out their frustration on the reader. Likewise, an access control system located at a boat marina or at a military facility in the desert will be subject to heat and moisture extremes that must be considered and tested before final acceptance.

While the physical aspects of reliability are important, they can usually be addressed by better material selection, manufacturing quality, and testing. What is often more difficult to determine during the research and product selection stage is the product's ability to work reliably and accurately over a long period of time. The product must have the ability to

minimize false positives and negatives, make accurate authentication and authorization decisions, follow organizational policies (as defined within the product) unambiguously, and function predictably according to the expectations of the organization. Reliability of the system is a fundamental requirement, for without it the organization cannot place any confidence in the system or its results. An access control system that fails may even cause a complete denial of service to the organization. The inability to trust in the accuracy and reliability of an access control system will cause the entire access control infrastructure to collapse.

Transparency

Security (more specifically, the implementation of most security controls) has long been a sore point with users who are subject to security controls. Historically, security controls have been very intrusive to users, forcing them to interrupt their work flow and remember arcane codes or processes (like long passwords or access codes), and have generally been seen as an obstacle to getting work done. In recent years, much work has been done to remove that stigma of security controls as a detractor from the work process adding nothing but time and money. When developing access control, the system must be as transparent as possible to the end user. The users should be required to interact with the system as little as possible, and the process around using the control should be engineered so as to involve little effort on the part of the user.

For example, requiring a user to swipe an access card through a reader is an effective way to ensure a person is authorized to enter a room. However, implementing a technology (such as RFID) that will automatically scan the badge as the user approaches the door is more transparent to the user and will do less to impede the movement of personnel in a busy area. In another example, asking a user to understand what applications and data sets will be required when requesting a system ID and then specifically requesting access to those resources may allow for a great deal of granularity when provisioning access, but it can hardly be seen as transparent.

A more transparent process would be for the access provisioning system to have a role-based structure, where the user would simply specify the role he or she has in the organization and the system would know the specific resources that user needs to access based on that role. This requires less work and interaction on the part of the user and will lead to more accurate and secure access control decisions because access will be based on predefined need, not user preference. When developing and implementing an access control system special care should be taken to ensure that the control is as transparent to the end user as possible and interrupts his work flow as little as possible.

Scalability

Setting up an access control system for five people can be hard. Setting up an access control system for 5,000—or 50,000—people is really hard. Ensuring the same system originally developed for five will work just as well for 50,000 can be next to impossible. When establishing an access control system, the security professional should always assume that the system will grow beyond original expectations and ensure the capacity of the technology and the process scales accordingly. Advances in cloud computing and "software as a service" has reduced scalability concerns from many organizations; however, prudent planning should be conducted to ensure an organization's information systems can accommodate future growth.

Several models and "rules" exist for capacity planning. These rules and models make certain assumptions about the industry, user base and type of information or processes the system supports. Information security professionals need to understand their industry, the types of information and processes they are supporting and what kind of growth or contraction can be expected in information system use.

Initial capacity estimates may suffice for a project's original needs and purposes, but the security professional should assume that the system will grow well beyond original estimates and should plan, as much as reasonably

possible, to ensure that any given solution has the ability to scale with that growth.

Integrity

Maintaining the integrity of the system includes many facets. Most notably, assuring that only authorized personnel have access to the administrative functions of the system. An attacker gaining the ability to manage the configuration of the access control system would have the ability to establish valid user credentials, alter or erase log and audit data, cause denial-of-service situations, or establish operational rules to selectively allow or deny users access to the protected system. Ensuring that only authorized personnel have access to administer the system goes a long way toward ensuring the integrity of the access control function. Regular testing of the access control function will ensure that the service maintains its integrity over time. As the system remains in continuous use it may begin to lose sensitivity, components may begin to wear out, or continuous administrative updates may introduce conflicts or obsolescence in the access rule set. Regular administrative care and testing will ensure that the system continues to operate within expected functional parameters and that any deviations from those parameters are caught early and corrected.

Maintainability

The access control system should require a minimum of maintenance to function properly over an extended period of time. Naturally, the physical components of the system may wear out over time, such as card readers, keypads, or support systems, and the cost and effort to maintain these components should be calculated into the overall business case for the system. However, the personnel effort to maintain the system should not be underestimated or overlooked.

Depending on the type of technology in use, the administrative effort required to keep the system in proper working order can be considerable or require specialized skills that may be expensive to acquire or maintain.

Overall, however, an effective access control system is one that requires a minimum of maintenance oversight or continuous tuning. Administrative effort and fine tuning should be concentrated on updating rule sets, managing user populations, and policy development. The management of these functions should also require as little effort as possible. The administrative controls over the system should be straightforward to understand and simple to operate. A system that is overly complicated to understand or difficult to maintain is one that will either quickly fall into disorder or be replaced with a system that is easier to manage.

Authentication Data Security

Equally as important as the access control system is to an organization are the controls that protect the authentication data itself. The authentication data include user identities, passwords, biometric information, access capabilities, and a host of other sensitive information which, if obtained by an attacker, would provide a roadmap for infiltrating and navigating around an organization's information systems. The protections around the authentication database should be researched and tested before the system is implemented. Data encryption should be in place, system- and file-level access controls should be present, and strong authentication for administrative functions should be investigated.

Auditability

Even if the access control system operates perfectly within expected parameters and there are no apparent instances of system failure or unauthorized access, a complete audit trail of system activities is necessary to provide documented assurance that the system is functioning properly. The system should have the ability to provide a complete record of all access control activity. This includes authentication requests, data access attempts, changes to privilege levels, and exercise of administrative capabilities. It is extremely important that this activity is recorded for successful activity as well as failures. Too often, systems record only failed instances of the above activity. Unfortunately, if an attacker succeeds in gaining authorized access

to the system, or if an authorized insider attempts to perform nefarious acts the system that only records event failures will fail to capture the activity of these individuals. This will lead to an inability to understand precisely what these individuals did within the system and a failure to properly investigate and prosecute (organizationally or legally) their activities.

Types & Categories of Access Controls

In the development of an access control architecture for an enterprise, it is necessary to fully understand the different categories and types of potential controls. This section will describe those different categories and discuss how each fits into the overall access control universe. This will also establish a foundation for later discussion on access control technology, practices, and processes.

There are literally hundreds of different access approaches, control methods, and technologies, both in the physical world and in the virtual electronic world. Each method addresses a different type of access control or a specific access need. For example, access control solutions may incorporate identification and authentication mechanisms, filters, rules, rights, logging and monitoring, policy, and a plethora of other controls. However, despite the diversity of access control methods, all access control systems can be categorized into seven primary categories. The seven main categories of access control are

1. ***Directive:*** Controls designed to specify acceptable rules of behavior within an organization
2. ***Deterrent:*** Controls designed to discourage people from violating security directives
3. ***Preventive:*** Controls implemented to prevent a security incident or information breach
4. ***Compensating:*** Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
5. ***Detective:*** Controls designed to signal a warning when a security control has been breached
6. ***Corrective:*** Controls implemented to remedy circumstance, mitigate damage, or restore controls
7. ***Recovery:*** Controls implemented to restore conditions to normal after a security incident

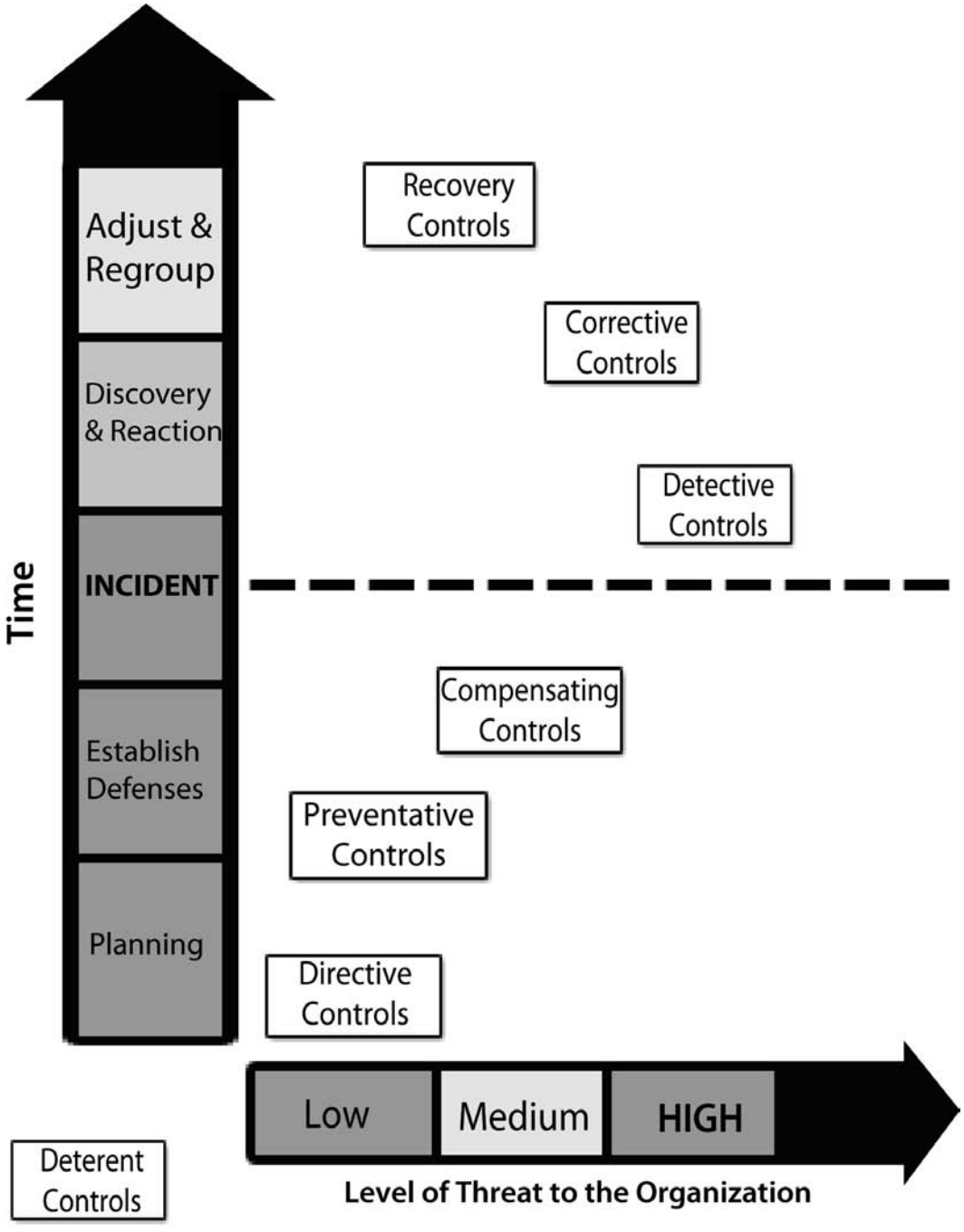


Figure 1.6 - **Continuum of controls relative to the time line of a security incident**

Figure 1.6 shows a continuum of controls relative to the time line of a security incident:

Directive Controls

Directive controls, sometimes referred to as administrative controls, provide guidance to personnel as to the expected behavior with respect to security within the organization. Directive controls provide users with the general guidelines they must follow if they are to be permitted access to information or systems. Directive controls are not only applicable to an organization's employees but contractors, guests, vendors, and anyone else who will have access to the organization's information systems must additionally abide by them.

The most common examples of directive controls are the organization's security policies and procedures. These documents provide the basis for information security throughout the organization and provide personnel with the model that must be adhered to as they perform their work. Although directive controls are generally implemented in the form of documented statements of organizational intent, they should not be considered optional or modifiable by organization personnel.

Directive controls have the weight of law within the organization and should be as strongly followed as any technical or procedural limitation. Many organizations compile their directive controls into a single acceptable use policy (AUP). The AUP provides a concise listing of the proper (and, in many cases improper) procedures, behaviors, and processes that all personnel must follow in order to gain and maintain access to information and systems within the organization. It is considered a best practice for all employees to agree to and sign the AUP before being granted access to any organizational resource. If the employee is unable (or unwilling) to abide by the terms of the AUP, no access will be granted. Many organizations require their employees to sign the AUP annually, either as part of the regular security awareness training or as part of the annual performance review process.

Deterrent Controls

Access controls act as a deterrent to threats and attacks by the simple fact that the existence of the control is enough to keep some potential attackers from attempting to circumvent the control. This is often because the effort required to circumvent the control is far greater than the potential reward if the attacker is successful, or, conversely, the negative implications of a failed attack (or getting caught) outweigh the benefits of success. For example, by forcing the identification and authentication of a user, service, or application, and all that it implies, the potential for incidents associated with the system is significantly reduced because an attacker will fear association with the incident. If there are no controls for a given access path, the number of incidents and the potential impact become infinite. Controls inherently reduce exposure to risk by applying oversight for a process. This oversight acts as a deterrent, curbing an attacker's appetite in the face of probable repercussions.

The best example of a deterrent control is demonstrated by employees and their propensity to intentionally perform unauthorized functions, leading to unwanted events. When users begin to understand that by authenticating into a system to perform a function, their activities are logged and monitored, and it reduces the likelihood they will attempt such an action. Many threats are based on the anonymity of the threat agent, and any potential for identification and association with their actions is avoided at all costs. It is this fundamental reason why access controls are the key target of circumvention by attackers. Deterrents also take the form of potential punishment if users do something unauthorized. For example, if the organization policy specifies that an employee installing an unauthorized wireless access point will be fired, that will deter most employees from installing wireless access points.

The effect deterrent controls have on a potential attacker will vary with both the type of control and the motivation of the attacker. For example, many organizations post a warning message to computer users during the

login process indicating that their activities may be monitored. While this may deter a casual user from performing unauthorized activities, it will not stop a determined attacker from his goals. Likewise, implementing a multifactor authentication mechanism on an application will greatly reduce system compromises through such mechanisms as password guessing, but a sophisticated attacker may then turn to the use of a vulnerability scanning tool to determine if the system can be compromised through a host or network vulnerability. As the sophistication and the determination of an attacker rises, so does the sophistication and cost of an effective deterrent to prevent that attacker from attempting his attack.

Preventative Controls

Preventative access controls keep a user from performing some activity or function. Preventative controls differ from deterrent controls in that the control is not optional and cannot (easily) be bypassed. Deterrent controls work on the theory that it is easier to obey the control rather than to risk the consequences of bypassing the control. In other words, the power for action resides with the user (or the attacker). Preventative controls place the power of action with the system, obeying the control is not optional. The only way to bypass the control is to find a flaw in the control's implementation.

Compensating Controls

Compensating controls are introduced when the existing capabilities of a system do not support the requirement of a policy. Compensating controls can be technical, procedural, or managerial. Although an existing system may not support the required controls, there may exist other technology or processes that can supplement the existing environment, closing the gap in controls, meeting policy requirements, and reducing overall risk. For example, the access control policy may state that the authentication process must be encrypted when performed over the Internet. Adjusting an application to natively support encryption for authentication purposes may be too costly. Secure Socket Layer (SSL), an encryption protocol,

can be employed and layered on top of the authentication process to support the policy statement. Other examples include a separation of duties environment, which offers the capability to isolate certain tasks to compensate for technical limitations in the system and ensure the security of transactions. In addition, management processes, such as authorization, supervision, and administration, can be used to compensate for gaps in the access control environment.

Keep in mind that it is typically not be possible to completely eliminate the risk in a given area while still allowing functionality. The use of compensating controls allows an organization to reduce that risk down to a level that is acceptable, or at least more manageable. Finally, compensating controls can be temporary solutions to accommodate a short-term change, or support the evolution of a new application, business development, or major project. Changes and temporary additions to access controls may be necessary for application testing, data center consolidation efforts, or even to support a brief business relationship with another company. The critical points to consider when addressing compensating controls are:

- Do not compromise stated policy requirements.
- Ensure that the compensating controls do not adversely affect risk or increase exposure to threats.
- Manage all compensating controls in accordance with established practices and policies.
- Compensating controls designated as temporary should be removed after they have served their purpose and another, more permanent control should be established.

Detective Controls

Detective controls warn when something has happened, and are the earliest point in the post-incident timeline. Access controls are a deterrent to threats and can be aggressively utilized to prevent harmful incidents through the application of least privilege. However, the detective nature of

access controls can provide significant visibility into the access environment and help organizations manage their access strategy and related security risk. As mentioned previously, strongly managed access privileges provided to an authenticated user offer the ability to reduce the risk exposure of the enterprise's assets by limiting the capabilities that authenticated user has. However, there are few options to control what a user can perform once privileges are provided. For example, if a user is provided write access to a file and that file is damaged, altered, or otherwise negatively impacted (either deliberately or unintentionally), the use of applied access controls will offer visibility into the transaction. The control environment can be established to log activity regarding the identification, authentication, authorization, and use of privileges on a system. This can be used to detect the occurrence of errors, the attempts to perform an unauthorized action, or to validate when provided credentials were exercised. The logging system as a detective device provides evidence of actions (both successful and unsuccessful) and tasks that were executed by authorized users.

Detection aspects of access control can range from evidentiary, such as post incident investigations, to real-time alerting of inappropriate activities. This philosophy can be applied to many different characteristics of the security environment. Access detection can be triggered by intrusion detection systems (IDSs), virus controls, applications, Web filtering, network operations, administration, logs and audit trails, and security management systems. Visibility into the environment is a key factor in ensuring a comprehensive security posture and the ability to promptly detect problems in the environment.

Corrective Controls

When a security incident occurs, elements within the security infrastructure may require corrective actions. Corrective controls are actions that seek to alter the security posture of an environment to correct any deficiencies and return the environment to a secure state. A security incident signals the failure of one or more directive, deterrent, preventative, or compensating

controls. The detective controls may have triggered an alarm or notification, but now the corrective controls must work to stop the incident in its tracks. Corrective controls can take many forms, all depending on the particular situation at hand or the particular security failure that needs to be dealt with.

The sheer number of corrective actions possible makes them difficult to successfully quantify. They can range from "quick fix" changes like new firewall rules, router access control list updates, and access policy changes to more long-term infrastructure changes like the introduction of certificates for wireless 802.1x authentication, movement from single-factor to multifactor authentication for remote access, or the introduction of smart cards for authentication. The difficulty in quantification is founded on the fact that access controls are universal throughout the environment. Nevertheless, it is important that a consistent and comprehensive management capability exists that can coordinate and employ corrective changes throughout the enterprise to enable policy compliance.

Recovery Controls

Any changes to the access control environment, whether in the face of a security incident or to offer temporary compensating controls, need to be accurately reinstated and returned to normal operations. There are several situations that may affect access controls, their applicability, status, or management. Events can include system outages, attacks, project changes, technical demands, administrative gaps, and full-blown disaster situations. For example, if an application is not correctly installed or deployed, it may adversely affect controls placed on system files or even have default administrative accounts unknowingly implemented upon install. Additionally, an employee may be transferred, quit, or be on temporary leave that may affect policy requirements regarding separation of duties. An attack on systems may have resulted in the implantation of a Trojan horse program, potentially exposing private user information, such as credit card information and financial data. In all of these cases, an undesirable situation must be rectified as quickly as possible and controls returned to normal operations.

	Directive	*Deterrent*	*Preventative*	*Detective*	*Corrective*	*Recovery*	*Compensating*
Administrative	Policy	Policy	User registration procedure	Review violation reports	Termination	DR Plan	Supervision
							Job rotation
							Logging
Logical	Config standards	Warning banner	Password based login	Logs	Unplug, isolate, & terminate connection	Backups	CCTV
			IPS	IDS			
							Keystroke monitoring
Physical	Authorized Personnel Only signs, traffic lights	Beware of Dog sign	Fence	Sentry	Fire extinguisher	Rebuild	Layered defense
				CCTV			

Figure 1.7 - **Control examples for types and categories.**

Access Control Types

The access control categories discussed in the previous section serve to classify different access control methods based on where they fit into the access control time continuum shown in *Figure 1.6*. However, another way to classify and categorize access controls is by their method of implementation. For any of the access control categories, the controls in those categories can be implemented in one of three ways:

- ***Administrative Controls:*** Sometimes called Management Controls, these are procedures implemented to define the roles, responsibilities, policies, and administrative functions needed to manage the control environment.
- ***Logical (Technical) Controls:*** These are electronic hardware and software solutions implemented to control access to information and information networks.
- ***Physical Controls:*** These are controls to protect the organization's people and physical environment, such as locks, fire management, gates, and guards. Physical controls may be called "operational controls" in some contexts.

The categories discussed earlier can be mapped against these three access control types to demonstrate various control examples and options as shown in *Figure 1.7*.

Physical Controls

Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier

in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area. For example, the fire control and suppression systems must account for the health safety of personnel in potential fire zones. One must consider fires, floods, explosions, civil unrest, or other man-made or natural disasters when planning the physical layout of a facility. Emergency strategies must be included in the physical controls to accommodate the safe exiting of personnel and adherence to safety standards or regulations. Adequate exits and emergency evacuation routes must be available in all areas and sensitive areas or information must be able to be secured quickly in case those areas must be evacuated. Human safety is the priority in all decisions of physical security.

The physical access controls in each zone should be matched with the level of security required for that zone. For example, an employee may work in the data center of a large financial institution—a very sensitive area. The employee may have a special badge to access the parking lot and the main entrance where guards are posted and recording access. To access the specific office area, he or she may need a different badge and PIN to dis-engage the door lock. Finally, to enter the data center, the card and PIN are combined with a biometric device that must be employed to gain access. As one gets closer and closer to the valuable asset—the data center—the protections get progressively stronger.

The most prevalent and visible aspect of physical security is often the perimeter of a facility. A typical perimeter should be without gaps or areas that can be easily broken into or entered undetected. The perimeter starts with the surrounding grounds. Hills, ditches, retention walls, fences, concrete posts, and high curbs can all act as deterrents to attack. Depending on the sensitivity of the facility, guards, attack dogs, and other aggressive measures can be applied. The construction of the facility may include

special walls, reinforced barriers, and even certain foliage strategically placed near doors, windows, and utilities. All this can be augmented by cameras, alarms, locks, and other essential controls.

However, security is not the only consideration when designing a facility. The overall design of the facility must balance function of the building with the security needs of the organization. For example, a company's headquarters building will need good security to protect private areas, stored records, and personnel against malicious acts. But it must also serve as the company's face to the public and present a welcoming atmosphere to visitors. Protections at such a facility might include guards at the front desk (unarmed), locked doors, and badge readers to restrict entry. However, the company's data center facility would most likely have much more stringent measures to keep intruders out, such as a tall razor-wire fence, armed guards, biometric entry controls, and mantrap doors. As with all architecture, form follows function.

If an organization leases space in a facility (as opposed to owning the facility) there may be limits on what modifications can be made to accommodate the company's security needs. Any special security requirements must be negotiated with the facility's owner before the lease agreement is signed. If the organization is sharing the facility with other tenants, additional thought must be given to security and access control measures, since much of the facility (those portions not occupied by the organization) will be accessible to non-organization personnel. Areas of special concern to the information security professional will include heating ventilation and air conditioning (HVAC) equipment, electrical power panels and wiring closets—all of which may be readily accessible to contractors and other tenants of the facility.

Finally, the oversight of physical controls must adhere to the same basic principles as other forms of controls: separation of duties and least privilege. For example, it may be necessary to segment the job role of various guards

to ensure that no single point of failure or collusion potentially allows threat agents to enter unchecked.

Physical Entry

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. The provisioning of credentials must take into consideration the needs of the individual, his or her job function, and the zone accessed. As discussed previously, the person requiring access must successfully pass an investigative process prior to being provided access. In defining physical entry controls, the following should be considered:

- Visitors should be appropriately cleared prior to entry and supervised while on the premises. Moreover, the date, time, and escort should be recorded and validated with a signature. Visitors should only be provided access to the areas that do not contain sensitive information or technologies and should be provided with instructions concerning security actions and emergency procedures.
- Access to controlled areas, such as information processing centers and where sensitive data may reside, should be restricted to authorized persons only. Authentication controls, such as badges, swipe cards, smart cards, proximity cards, PINs, and (potentially) biometric devices, should be employed to restrict access.
- Everyone within the controlled perimeter must wear some form of identification and should be encouraged to challenge others not wearing visible identification. Be aware, however, that most cultures encourage politeness and deference in social interactions, particularly where strangers are involved. Challenging an unknown person does not come easily to many people and this may be a large culture change for most organizations. Awareness and education programs on this topic are advised.
- Different styles of identification should be employed to allow others to quickly ascertain the role of an individual. For

example, employees may be given white badges and visitors given blue badges. This makes it easier to identify who is an employee and who is not to ensure that all nonemployees are escorted in the building. In another example, a red ID badge may signify access to the fourth floor of an office building. If someone appeared on the fourth floor wearing a blue badge, others would be able to determine appropriate actions. Action may include verifying they are escorted, notifying security, or escorting them to the nearest exit.

- All access rights and privileges should be regularly reviewed and audited. This should include random checks on seemingly authorized users, control devices, approval processes, and training of employees responsible for physical security.

There may be occasional need for temporary facility access to sensitive areas for visitors, contractors, or maintenance personnel. Preparations and procedures should be defined in advance for these situations; special identification should be required for all temporary personnel, and they should be escorted by facility personnel at all times. This will make it easier for regular facility personnel to identify the temporary visitors in unauthorized areas and ensure that they are not able to cause any damage to the facility or obtain any confidential information.

Administrative Controls

Administrative controls represent all the actions, policies, processes, and management of the control system. These include any aspect of the access control environment that is necessary to oversee and manage the confidentiality, availability, and integrity of the access controls, and manage the people who use it, set policy on use, and define standards for operations.

Administrative controls can be broad and can vary depending on organizational needs, industry, and legal implications. Nevertheless, they can be broken into six major groups:

- Policies and procedures
- Personnel security, evaluation, and clearances
- Security policies
- Monitoring
- User management
- Privilege management

Policies and Procedures

The first aspect of administrative (managerial) oversight is the operations management of the control environment and how it should align with the enterprise architecture. Access control is realized by aligning the capabilities of many systems and processes, collaborating to ensure that threats are reduced and incidents prevented. Therefore, other operational elements of the environment must be addressed in some fashion within the access control strategy. These include but are not limited to:

- Vulnerability management and patch management
- Product life-cycle management
- Network management

When changes to the environment are required to accommodate a need, they must be defined, approved, tested, applied, verified, deployed, audited, and documented. Changes can be minor, such as a static route being added to a network, or more significant, such as the redesign of a storage solution. Every organization must have a change control process to ensure that there is a formalized methodology for making and documenting changes to the environment.

Given the scope of access control, it is important that the change control process includes aspects of the access strategy and policy. In some cases, this is obvious, such as adding a new virtual private network (VPN) gateway for remote access. Clearly this will affect the access control environment. Some changes, such as network redesign, which can affect

various established access paths to information, are much less obvious, but can have significant impacts to access controls.

Many organizations have business continuity and disaster recovery (BCP/DRP) plans to ensure that the organization can maintain critical operations in case of a catastrophic event or failure. BCP/DRP plans can be simplistic, such as ensuring there are regular backups performed, or highly complex solutions incorporating multiple data centers. The scope and complexity of the BCP/DRP plan are typically defined by the business environment, risks, and system criticality.

Regardless of the type of BCP/DRP plan, the availability of access controls during an event is essential and must be incorporated into the plan. For example, if a system failure occurs and an alternate system is temporarily employed without the expected, original controls, the exposure to critical data can be significant. All too often, security is a secondary consideration in disaster recovery operations. If an event was to occur, a company could have its most valuable assets completely exposed. However, critical systems are most important in the context of BCP/DRP. Therefore, a system included in the BCP/DRP plan is important and the information on that system is valuable.

One of the first steps to ensure security incorporated into the BCP/DRP plan is defining the access controls for the temporary systems, services, and applications to be used during disaster recovery. This includes the access control system itself. For example, a Remote Authentication Dial In User Service (RADIUS) server may seem unimportant on the surface, but its absence in a disaster could be detrimental to security. In addition, a disaster scenario, by definition, is an unusual event with many extenuating arrangements that will need to be made to enable the organization to continue its work. Subsequently, there may be different access needs defined than what the organization would normally have in place. The notion of "acceptable security" may be very different during a disaster

than it would be under ordinary circumstances, so proper planning and consideration of alternative access control needs and methods must be considered and incorporated into the BCP/DRP plan.

Traditional networks and applications are typically engineered to provide a high level of performance to users, systems, and services. The network is the cardiovascular system of most companies, and if its performance is low, the productivity of the organization will suffer. The same holds true for the access control environment. If it takes a user an excessive amount of time to logon, this could have a negative impact to operations and potentially encourage users to find ways to bypass the access control system. To reduce the time associated with access controls, the performance optimization processes for the network and system environments should include the performance of controls overseeing authentication and access.

Like change control, configuration management represents the administrative tasks performed on a system or device to ensure optimal operations. Configurations can be temporary or permanent to address a multitude of the organization's operations and security needs, and configuration management of devices, systems, services, and applications can greatly affect the access control environment. Changes to a system's configuration must take into account what, if any, impacts on user access may occur after the configuration is modified.

Given the common separation of the security group from the IT group, it is not uncommon for the IT group to make a seemingly innocuous modification to a system configuration and impact the access controls associated with that system. Therefore, it is important to ensure that the resources responsible for configuration management, such as network administrators, system owners, and application developers, are aware of the security control environment and the importance of their domain of influence on the security of the organization. This often ties in closely with any change management processes an organization might have in place, so it is a

natural fit for processes to be enacted that tie in access control considerations as part of any change management or configuration management program.

Vulnerability management will typically include activities such as identifying system vulnerabilities, recommending potential remediation, and implementing system patches to accommodate a security issue, update a system service, or add features to a system or application. When patches are installed, there may be key system modifications that can negatively affect the security of the system, server, or application. Patches must be applied through the change control system to provide a comprehensive record of system modifications and accurate documentation. Ensuring that the current state of a system is well-documented allows organizations to gain more visibility into the status of their environment in the event a new vulnerability is published. This promotes rapid assessments to evaluate potential risks in the face of an attack or vulnerability. In addition, data from the change control system utilized during the application of patches offer documentation of the current state of a system that can be consulted prior to applying new patches or installing new software.

A key attribute of vulnerability management is the importance of minimizing the time for deploying patches or other system updates in order to mitigate a vulnerability. Vulnerabilities surface in a multitude of ways. For example, a vulnerability may be published by a vendor who has discovered a security issue and provides a patch. Usually, at this point, both attackers and organizations are made aware of the vulnerability. While companies are exercising due diligence in applying fixes, attackers are developing methods and tools to exploit the vulnerability. In contrast, an incident may have occurred that exposes the vulnerability in a system and constitutes an immediate threat. The most dangerous example of this kind of threat is zero day attacks, where an attacker identifies and exploits the vulnerability before that vulnerability is known to the vendor or the general user community. The attackers can exploit the vulnerability on a massive scale, understanding that time is on their side. It is very common

for attackers to discover a vulnerability, develop tools and tactics to exploit it, then execute those exploits before anyone knows of the vulnerability or how to defend against it. Vulnerable organizations must find alternative measures to compensate for the threat while vendors rush to produce a patch, each consuming time as the attacks expand.

Given the complexity of each potential scenario, time is always a critical element in protecting assets. The ability to use time effectively to deploy a patch or employ compensating controls until a patch is published directly corresponds to the level of risk and the overall security posture of the organization. Emphasis on efficient testing and deployment of system patches or compensating controls should be the core of any vulnerability management program.

However, time must be balanced against effective deployment. Initially, the documentation provided by the configuration management and change control processes can be investigated to determine which systems are vulnerable and represent the greatest risk, then prioritized accordingly. As the process continues, other affected systems are addressed by a manual or automated (or combination) patch management process that is used to deploy the update throughout the organization. The vulnerability management program must then verify that the patch was, in fact, implemented as expected. Although this may seem inherent to the objective, it cannot be assumed. In the case of manual deployment, users and system owners may not respond accordingly or in a timely fashion. Even if timely deployment is executed, the patch may have failed. This is somewhat compensated for in automated deployment; nevertheless, both scenarios require validation of an effective installation.

The installation of a patch or control does, by itself, represent the complete mitigation of an identified vulnerability. Many systems are unique to a specific environment, representing the potential that a change mitigating one vulnerability unintentionally introduces another. Or, in some cases, it is assumed that the implementation of a patch or control eliminated the

vulnerability altogether. Therefore, a vulnerability management system must not only address the testing, deployment, and verification that the patch was implemented as expected, but also include testing to ensure that the target vulnerability was mitigated and new problems were not introduced by the process. In the final analysis, vulnerability management is a comprehensive and integral process that every security program must develop, maintain, and test regularly.

In every organization there comes a time to upgrade or replace devices and systems. Reasons for the upgrade vary, but can include product obsolescence, the availability of newer technology with previously unavailable desirable features, or the need for advanced operational capabilities. Baselines must be established within the access control architecture that define the minimum access control requirements for all new systems to ensure that appropriate and acceptable controls are established. By doing so, the organization has a clear foundation by which to evaluate products for implementation without sacrificing security or expected controls. Do not assume that all new products have the security capabilities the organization needs. Each organization's needs vary and each environment may be different from that for which the product was designed. It is important to test all new products for access control functionality.

Finally, many networks are supported by a separate management network that allows administrators to manage devices without affecting the production environment. This is another form of separation of duties, where the production network and the management network have separate purposes, separate network connectivity, and separate access and control requirements. Given the ability to change aspects of the network environment, it is necessary to have strong access controls established on the management network to reduce risk to systems and network devices. If network management is performed using the same network as general production traffic, strong authentication and authorization are required to ensure that unauthorized personnel cannot modify network devices.

Personnel Security, Evaluation, and Clearances

One of the more overlooked aspects of access control is a review of the requirements of people requesting access to a resource. Prior to granting access of any kind, the credentials of the person requesting the access should be checked for validity and his need for access thoroughly evaluated. This does not mean that every user needs to have a complete background check prior to checking her e-mail. Clearly, the level of validation of an individual should be directly proportional to the sensitivity of the assets and the level of permissions available to the user. Nevertheless, it is critical that processes exist to evaluate users and ensure that they are worthy of the level of trust that is requested and, ultimately, granted.

First and foremost, security requirements—at some level—should be included in all defined job roles and responsibilities. Job roles defined by the organization should have alignment to defined policies and be documented appropriately. They should include any general responsibilities for adhering to security policies, as well as any specific responsibilities concerning the protection of particular assets related to the given role.

Once the security requirements for a role are defined and clearly documented, the process for validation of individuals to obtain credentials for a role can be defined and exercised. The definition of a screening process is typically related to the sensitivity of the assets being accessed. However, there may be contractual demands, regulatory compliance issues, and industry standards that define how a person is screened to reach a certain level of access. The best example of this type of screening comes from the military and the allocation of clearances. Depending on the clearance level requested, a person may be subjected to intense background checks, friend and family interviews, credit checks, employment history, medical history, polygraph examinations, and a plethora of other potentially unpleasant probing. Of course, once attained, the clearance translates to a level of trustworthiness and, therefore, access.

A typical organization will need only a standard process and some additional factors in the light of applicable legal requirements or regulations. These may include a credit check and criminal background checks that simply assure management that an applicant has not falsified information during the application process. Typical aspects of staff verification may include but are not limited to:

- Satisfactory character references
- Confirmation of claimed academic and professional qualifications
- Independent identity validation, such as a passport
- A credit check for those requiring access to financial systems
- Federal, state, and local law enforcement records check
- An online search of publicly available information on social media sites

The relevance of credit checks and other personal history can be valuable in determining a person's propensity for unlawful acts. Personal or financial problems, changes in behavior or lifestyle, recurring absences, and evidence of stress or depression might lead an employee to fraud, theft, error, or other security implications. The type of background check performed may vary based on the type of employee and his or her placement in the organization. For example, a file clerk or receptionist may need only a basic background check, whereas an applicant for a senior officer position may require a more extensive background investigation.

In the event the employee is temporary, the access provided must take into consideration the potential exposure of proprietary information given the transient position. Organizations that use staffing agencies to supply temporary help should require those agencies to perform employee validation checks and provide a reliability report on the temporary workers supplied to the organization. The requirements for background checks should be incorporated into the underlying contract with the

staffing agency and its implementation should be reviewed and audited on a regular basis. Management should also evaluate the supervision and provisioning of access to new or inexperienced staff. It should not be necessary to provide a new employee with the keys to the kingdom until he or she has satisfied a probationary period.

Employees should also be periodically reevaluated to ensure that significant changes to key elements about them or their lives have not occurred that would alter their security worthiness. Also, it is important to remember that all information collected about an individual is private and confidential and should be afforded security controls like any other sensitive material. Finally, confidentiality or nondisclosure agreements should be read and signed annually by all employees to ensure there is no doubt on the part of employees that the information they will have access to is confidential, secret, protected, and valuable to the organization.

Security Policies

The organization's requirements for access control should be defined and documented in its security policies. Access rules and rights for each user or group of users should be clearly stated in an access policy statement. The access control policy should minimally consider:

- Statements of general security principles and their applicability to the organization
- Security requirements of individual enterprise applications, systems, and services
- Consistency between the access control and information classification policies of different systems and networks
- Contractual obligations or regulatory compliance regarding protection of assets
- Standards defining user access profiles for organizational roles
- Details regarding the management of the access control system

Monitoring

The ability to monitor the access control environment effectively is essential to the overall success and management of the security program. It is one thing to apply controls, but it is another to validate their effectiveness and ongoing status. The capacity for ensuring that controls are properly employed and working effectively and for being aware of unauthorized activity is enabled by the existence of monitoring and logging within the environment. This is not unique to access controls, security, or even IT; it is an essential aspect of business to monitor activity.

Systems should be monitored to detect any deviation from established access control policies and record all successful and unsuccessful authentication processes, credential assertion, user management, rights usage, and access attempts. The procedures and technology should also monitor the ongoing status of controls to ensure conformity to policies and expectations. This last point is typically overlooked and represents a significant potential to mask or hide unauthorized activities. For example, if the control activities are monitored, yet the status of controls is not, attackers can disable various controls, grant themselves access, and then re-enable the controls without detection. The logging and monitoring of the activities will then not raise any suspicion because they are now valid operations, thanks to the attacker.

Systems and activity logs are (typically) electronic records of any activity that has occurred within a system or application. They provide the documented record of what has happened and can be extremely useful when investigating an operational or security incident. Logs and their contents are important to security management and maintenance of an effective access control solution. A log can include:

- User IDs used on systems, services, or applications.
- Dates and times for logon and logoff.
- System identities, such as IP address, host name, or media access control (MAC) address. It may also be possible to

determine the network location of a device through local area network (LAN) logging, wireless access point identification, or remote-access system identification, if applicable.

- Logging of both successful and rejected authentication and access attempts. Knowing when and where people are utilizing their rights can be very helpful to determine if those rights are necessary for a job role or function. It is also helpful to know where access rights are denied to have a better understanding of what a user is trying to do. This can help determine if you have a user who does not have adequate rights to perform his or her job.

Audit logs should be retained for a specified period, as defined by organizational need and (potentially) regulatory requirements. In the latter case, this is preordained and not open to interpretation. However, there are cases where no legal or regulatory demands exist. If this is the case, the retention time will probably be defined by organizational policy and the size of available storage. The security of the logs is critical. If a log can be altered to erase unauthorized activity, there is little chance for discovery, and if discovered, there may be no evidence. Logs must also be protected from unauthorized reading as well as writing, as they can contain sensitive information such as passwords (for instance, when users accidentally type the password into a user ID prompt). Log security is also critical if the logs are needed as evidence in a legal or disciplinary proceeding. If logs are not secure and can be proven as such before, during, and after an event, the logs may not be accepted as valid legal evidence due to the potential for tampering. The fundamental approach to logs is that they must be an accurate reflection of system activity and, as such, must be secured and maintained for an appropriate period of time in order to provide a reference point for future investigative activity.

Once the events are properly logged, it is necessary to periodically review the logs to evaluate the impact of a given event. Typically, system logs are voluminous, making it difficult to isolate and identify a given event for identification and investigation. To preserve potential evidence,

many organizations will make a copy of the log (preserving the original) and use suitable utilities and tools to perform automated interrogation and analysis of the log data. There are several tools available that can be very helpful in analyzing a log file to assist administrators in identifying and isolating activity. Once again, separation of duties plays an important role in reviewing logs. Logs should never be initially reviewed or analyzed by the "subject" of the logs. For example, a system administrator should not perform the log review for a system he manages. Otherwise, it may be possible for the person to "overlook" evidence of her unauthorized activity or intentionally manipulate the logs to eliminate that evidence. Therefore, it is necessary to separate those being monitored from those performing the review.

User Access Management

An organization must have a formal procedure to control the allocation of credentials and access rights to information systems and services. The procedure should cover all stages in the life cycle of user access, from the initial registration of new users to the final decommissioning of accounts that are no longer required. To provide access to resources, the organization must first establish a process for creating, changing, and removing users from systems and applications. These activities should be controlled through a formal process, based on policy, which defines the administrative requirements for managing user accounts. The process should define expectations, tasks, and standards concerning the user management. For example, elements of the process should include:

- Approval of user access, including information from human resources, the user's manager, or a business unit that has approved the creation of the user account. The owner of the system who is providing information or services should concur with the approval request. Approval processes should also address the modification of user accounts and their removal.
- Standards defining unique user IDs, their format, and any application-specific information. Additionally, information

about the user should be included in the credential management system to ensure the person is clearly bound to the user ID defined within the system.

- A process for checking that the level of access provided is appropriate to the role and job purpose within the organization and does not compromise defined segregation of duties requirements. This is especially important when a user's role and job function change. A process must exist to evaluate existing privileges compared to the new role of the user and ensure changes are made accordingly.
- Defining and requiring users to sign a written statement indicating that they understand the conditions associated with being granted access and any associated liabilities or responsibilities. It is important to understand that user confirmation should occur whenever there is a change in rights and privileges, not simply upon creation of the account.
- A documentation process to capture system changes and act as a record of the transaction. Keeping a log of the administrative process and relative technical information is essential to an effective access control system. The information will be used in assessments, audits, change requests, and as evidence for investigative purposes.
- Access modification and revocation procedures to ensure that users who have left the organization or changed job roles have their previously held access privileges immediately removed to ensure elimination of duplications and removal of dormant accounts.
- Specific actions that may be taken by management if unauthorized access is attempted by a user or other forms of access abuse are identified. This must be approved by the organization's human resources and legal departments.

A more in-depth look at user management will be found later in this chapter when identity management is discussed.

In addition to overall user management, it is necessary to define policies,

procedures, and controls regarding passwords. The use of passwords is a common practice for validating a user's identity during the authentication process. Given that, in most traditional authentication solutions, the password is the only secret in the transaction, great care should be considered in how passwords are created and managed by users and systems.

A process governing user password should consider the following:

- Users should be required to sign a statement agreeing to keep their passwords safe and confidential and to not share, distribute, or write down their passwords.
- All temporary passwords should be permitted to be used only once—to reset the user's password to something that only he or she knows.
- Passwords should never be stored unprotected and in clear text.
- Passwords should have a minimum and maximum length and require the use of various characters and formats to increase their complexity and reduce their susceptibility to brute force and guessing attacks.
- Passwords should be changed regularly.
- Accounts should be locked for a period of time if excessive failed password attempts occur (typically within three to five tries).
- A history of passwords should be maintained to prevent users from repeating old passwords as they are changed.
- Passwords should not be disclosed to support personnel, and those personnel should not ask users for their passwords.

There is some debate over the security realized by a username and password combination used for authentication. For example, depending on the system, a longer, more complex password can actually make it more prone to compromise if it results in the user writing it down. The potential for exposure of passwords, poor password selection by users, and the sheer

number of passwords most users need to track lay the foundation for potential compromises.

However, alternatives to passwords (such as will be examined later in this chapter) can be expensive, cumbersome, and annoying to end users, potentially negating any security or business benefit they may provide. Before moving away from the use of passwords toward an alternative technology or method, the security professional must always consider the value of the information or system that the passwords are protecting. Current password technology and processes (including the use of minimum complexity standards, lockouts, and reuse restrictions) will provide the organization with a certain minimal level of security protection. If, in the opinion of the organization, that level of protection is sufficient to protect the resources behind the password, then password technology is sufficient. If, however, the organization feels that password protection does not adequately protect the resources behind the password, then it must seek out alternative authentication methodologies.

Nevertheless, and despite all the negative connotations passwords have in the security space, passwords are today's de facto baseline standard. The best approach to ensure consistency and control is:

- Clearly defined password policies
- Well-implemented system controls
- Understanding of the technical considerations
- Comprehensive user training
- Continuous auditing

Privilege Management

The importance of access privileges demands that their allocation, administration, and use should have specific processes and considerations. The lack of effective privilege management can result in core failures in otherwise sophisticated access control systems. Many organizations will

focus exclusively on identification, authentication, and modes of access. Although all these are critical and important to deterring threats and preventing incidents, the provisioning of rights within the system is the next layer of control. The typical cause of problems in the allocation of rights is due primarily to the vast number of access options available to administrators and managers. The complexity of potential access configurations leads to inadequate and inconsistent security. This aspect of privilege management demands clear processes and documentation that defines and guides the allocation of system rights.

In the development of procedures for privilege management, careful consideration should be given to the identification and documentation of privileges associated with each system, service, or application, and the defined roles within the organization to which they apply. This involves identifying and understanding the available access rights that can be allocated within a system, aligning those to functions within the system, and defining user roles that require the use of those functions. Finally, user roles need to be associated with job requirements. A user may have several job requirements, forcing the assignment of several roles and result in a collection of rights within the system. Be careful, however, of the consequences of aggregate access rights. Many systems have rules of precedence that dictate how access rules are applied. Should a rule that restricts access conflict with, and be overridden by, a rule that allows access, the unintended consequence is that the user will be granted more access permission than was intended. Remember the primary mantra of least privilege: only rights required to perform a job should be provided to a user, group, or role.

An authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete and validated. If any significant or special privileges are needed for intermittent job functions, these should be performed using an account specifically allocated for such a task, as opposed to those used for

normal system and user activity. This enables the access privileges assigned to the special account to be tailored to the needs of the special function rather than simply extending the access privileges associated with the user's normal work functions. For example, an administrator of a UNIX system might have three accounts: one for daily routines, another for specific job requirements, and "root" (the all-omniscient access ID on UNIX systems) for rare occurrences where complete system access must be utilized.

Logical (Technical) Controls

Logical controls are those mechanisms employed within the digital and electronic infrastructure of an organization that enforce that organization's security policy. Given the pervasive nature of technology, logical access controls may take on a wide variety of forms and implementations. Logical controls can include elements such as firewalls, filters, operating systems, applications, and even routing protocols. Logical controls can be broadly categorized in the following groups:

- Network access
- Remote access
- System access
- Application access
- Malware control
- Encryption

Network Access

Network access controls are those employed within the communication infrastructure to restrict who may connect to, and use, that infrastructure. Usually, this is implemented through access control lists, remote-access solutions, virtual local area networks (VLANs), access control protocols, and security devices like firewalls and intrusion detection or intrusion prevention systems. The role of network access controls is usually to limit communications between two networks or resources. For example, a firewall will limit what protocols and protocol features are permitted from a given source to a defined destination.

However, there are other network-level controls that can be used to employ security services that increase the level of access management in the environment. The most common example is a proxy system: a device or service that is located in the middle of the communication between a user and an application and employs controls that monitor and regulate the traffic between the user and the application. Proxy systems can apply specific logic in managing service-level communications within the network. For example, a proxy system may control access to Web-based services via the hypertext transfer protocol (HTTP). Just as a firewall would block specific ports, a proxy system would block or control certain aspects of the HTTP session to limit exposure. Many proxy systems are used to authenticate sessions for internal users attempting to access the Internet and potentially filter out unwanted Web site activity, such as Java applets, active server page (ASP) code, plug-ins, or access to inappropriate Web sites.

VLANs can be utilized to segment traffic and limit the interaction from one network to another. VLANs are used in situations where many systems are on the same physical network but they need to be logically separated to enforce the access control requirements of the organization. Conversely, VLANs can be used to virtually connect systems in multiple physical locations to appear as if they are all on the same logical network segment.

Wireless networks can also employ several access control mechanisms, such as MAC filtering, multiple forms of authentication, encryption, and limitations on network access.

Network Access Control (NAC) provides is the ability to restrict access to systems based on network-wide policy. Prior to allowing a system to join the network, the NAC service queries the system to ensure it is adhering to established policies. Policies can be as simple as ensuring an antivirus package is present on the system and as complex as validating the system

is up to date with security patches. In the event the system does not meet security policy, it may be denied access or redirected to a secure area of the network for further testing or to allow the user to implement the necessary changes required prior to gaining full access the network.

Remote Access

In today's environment, users working from outside the traditional office space make up a significant portion of the user community. Remote access solutions offer services to remote users requiring access to systems and data. One of the more commonly utilized technical solutions is the virtual private network (VPN). VPNs allow users to authenticate themselves and establish a secure communications channel over an insecure medium like the Internet. Typically, a VPN device is placed on the organization's Internet connection or behind a firewall to allow remote users to access the network, authenticate, and establish a protected session with various internal systems.

VPN access controls typically use authentication mechanisms in combination with encryption methods. For example, a VPN solution can be configured to permit access by users with the appropriate specific (company branded) client software or version of a browser, limit access to certain portions of the network, limit the types of services permissible, and control session time windows. In addition, because the connection is occurring over an insecure and publicly accessible network like the Internet, most VPN solutions employ multifactor authentication to positively identify the user. Multifactor authentication will be covered in more detail later in the chapter.

System Access

The term "system" comprises a wide variety of technologies and components, but the definition most often used is one or more computers that provide a service or assist in a process. When most people think of a system they think of their personal computer, and that provides a

good model for discussing system access controls. The most prevalent system access control is the user ID and password combination. Almost all modern systems have this unless it has been specifically disabled for a particular reason. The user ID/password combination may be replaced in some systems by other forms of authentication, such as a smartcard or a one-time password token. Nevertheless, all these methods serve the same purpose: to restrict system access to authorized users.

All computer systems have an underlying operating system that controls all its functions and regulates how the various components of the system interact. There are literally hundreds of different operating systems, but most users (including security professionals) work primarily in one of the three major publicly available operating systems: Microsoft Windows®, Apple's OS X, and UNIX (including the many variants of Linux and OS X). Mobile operating systems such as Google's Android and Apple's iOS are also quickly becoming operating systems security professionals must be familiar with. Each of these operating systems has internal controls and layers built in that manage access control between components of the system. In particular, they all tightly control programs that directly access the hardware components of the system, such as the kernel (the part of the system that interfaces between the OS and the system hardware) and various device drivers that allow application programs to use devices like key-boards and printers. The ability to directly manipulate the system hardware is a powerful tool and must be tightly controlled by the operating system to prevent misuse by malicious programs.

Finally, almost all operating systems have some sort of file system to store information for later retrieval. The file system will also have controls to restrict who may access various files and directories. Some of these controls are imposed by the operating system itself, while others may be assigned by individual users to protect their personal files. These controls are very important to ensure that information is not disclosed to unauthorized individuals who may have access to the system.

Application Access

Applications will usually employ user and system access controls to deter threats and reduce exposure to security vulnerabilities. However, applications can also incorporate mechanisms to supplement other controls and ensure secure operations. For example, applications can monitor user sessions, apply inactivity time-outs, validate data entry, and limit access to specific services or modules based on user rights and defined user roles. Moreover, the application itself can be designed and developed to reduce exposure to buffer overflows, race conditions (where two or more processes are waiting for the same resource), and loss of system integrity.

The architecture of an application plays a significant role in its ability to thwart attack. Object-oriented programming, multitiered architectures, and even database security are important to controlling what services are provided to users and what tasks can be performed. Access controls associated with all aspects of an application are important to sound security. Many applications are complicated and offer a wide range of services and access to potentially sensitive information. Additionally, applications may be critical to the operational needs of the business. Therefore, their sensitivity to disruption must be considered when designing or using the access control features of the application.

Applications can also be segmented into modules or layers to further enforce access control policies. For example, a typical e-mail application can be segmented into modules for composing a message, managing address book information, connecting to net-work resources, and managing mail delivery and retrieval. Doing this allows the application designer to specify how each module can be accessed, what services each module will present to the user and to other applications, and what privileges each provides to the user. For example, the address book management module may be accessible from an e-mail application but not by any other application to prevent the possibility of a virus examining and using a user's address book. It is important to manage the interaction between application modules

within an application as well as the interaction between these modules and other applications to ensure that malicious users or programs do not try to use them to perform unauthorized activities. A more detailed discussion of application security issues is found in Chapters 4 and 6.

Malware Control

Malicious code, such as viruses, worms, Trojans, spyware, and even spam, represent potential security threats to the enterprise. Weaknesses in systems, applications, and services offer opportunities for worms and viruses to infiltrate an organization, causing outages or damage to critical systems and information. Technical controls can be applied to reduce the likelihood of impact from such malicious programs. The most prevalent of these controls are antivirus systems that can be employed on the network perimeter, servers, and end-user systems to detect and potentially eliminate viruses, worms, or other malicious programs. Other technical solutions include file integrity checks and intrusion prevention systems that can detect when a system service or file is modified, representing a risk to the environment.

Cryptography

Although covered in greater detail in the cryptography chapter of this book, encryption has an important role in the access control domain. Encryption can be used to ensure the confidentiality of information or authenticate information to ensure integrity. These two characteristics are highly leveraged in the identification and authentication processes associated with access control. Authentication protocols will employ encryption to protect the session from exposure to intruders, passwords are typically hashed (put through a one-way mathematical function that cannot be reversed) to protect them from disclosure, and session information may be encrypted to support the continued association of the user to the system and services used. Encryption can also be used to validate a session. For example, a server can be configured such that if session information is not encrypted, the resulting communication is

denied. The most predominant aspect of cryptography in access control is the employment of cryptographic mechanisms to ensure the integrity of authentication protocols and processes.

Encryption can also be used as a compensating control to improve security when the available access control functions are not granular enough to provide adequate security. For example, it may be necessary for several employees of a company to share a particularly sensitive financial spreadsheet. Unfortunately, all of these people are located in different offices in different parts of the country, and the only way for them to share this file is to use the company's general shared drive that was set up for all employees to transfer information between offices. While access to the drive is restricted to only internal company users, there is no way to specify that only particular users can access a specific file. In this case, the file can be encrypted and the key to decrypt the file can be disclosed only to the employees who need to see the spreadsheet. This will allow the file to be placed on the general shared drive while still restricting access to only those who need to see the file.

Cryptography is commonly used within applications to protect sensitive data. Information such as credit card numbers may be encoded so that they are not visible (except perhaps the last few digits) to personnel who do not need to see the entire number. Examples of this may be seen in reports or printouts, in the storage of such information in a database, or in the layout of a screen that is displayed to the user. Consider the use of encryption in those situations where the available access controls are not sufficient to provide the appropriate granularity of protection for sensitive information.

Access Control Techniques

Thus far in the chapter the discussion of access controls has been relegated to the processes and technology used to identify, authenticate, and authorize users and applications. However, all this must translate into specific controls associated with the security of data. In a defense-in-depth environment each layer of defense requires its own access controls and security capabilities.

Defining security controls for the systems and applications that host data is a good start, but special attention must also be paid to methods of organizing and protecting the data itself. This section will discuss various methods of providing data-based protection.

Discretionary and Mandatory Access Controls

One of the most fundamental data access control decisions an organization must make is the amount of control it will give system and data owners to specify the level of access users of that data will have. In every organization there is a balancing point between the access controls enforced by organization and system policy and the ability for information owners to determine who can have access based on specific business requirements. The process of translating that balance into a workable access control model can be defined by three general access frameworks:

- Discretionary access control
- Mandatory access control
- Nondiscretionary access control

Discretionary Access Controls (DACs)

Controls placed on data by the owner of the data. The owner determines who has access to the data and what privileges they have. Discretionary controls represent a very early form of access control and were widely employed in VAX, VMS, UNIX, and other minicomputers in universities and other organizations prior to the evolution of personal computers. Today, DACs are widely employed to allow users to manage their own

data and the security of that information, and nearly every mainstream operating system, from Microsoft and Apple to mobile operating systems and Linux supports DAC. The advantage of a DAC-based system is that it is primarily user-centric. The data owner has the power to determine who can (and cannot) access that data based on the business requirements and constraints affecting that owner. While the owner never has the ability to ignore or contradict the organization's access control policies, he or she has the ability to interpret those policies to fit the specific needs of his or her system and his or her users.

Mandatory Access Controls (MACs)

Controls determined by the system and based primarily on organization policy. The system applies controls based on the clearance of a user and the classification of an object or data. With DACs the user is free to apply controls at their discretion, not based on the overall value or classification of the data. In contrast, MAC requires the system itself to manage access controls in accordance with the organization's security policies. MACs are typically used for systems and data that are highly sensitive and where system owners do not want to allow users to potentially contradict or bypass organizationally mandated access controls. Assigning the security controls of an object based on its classification and the clearance of subjects provides for a secure system that accommodates multilayered information processing.

MAC is based on cooperative interaction between the system and the information owner. The system's decision controls access and the owner provides the need-to-know control. Not everyone who is cleared should have access, only those cleared and with a need to know. Even if the owner determines a user has the need to know, the system must ascertain that the user is cleared or no access will be allowed. To accomplish this, data need to be labeled as to its classification, allowing specific controls to be applied based on that classification.

Access Capabilities	
No Access	No access permission granted
Read (R)	Read but make no changes
Write (W)	Write to file. Includes change capability
Execute (X)	Execute a program
Delete (D)	Delete a file
Change (C)	Read, write, execute, and delete. May not change file permission.
List (L)	List the files in a directory
Full Control (FC)	All abilities. Includes changing access control permissions.

Access Permissions	
Public	R - L
Group	R - X
Owner	R - W - X - D
Admins	FC
System	FC

Figure 1.8 **- An example of access permissions. Access permissions are applied to an object based on the level of clearance given to a subject.**

As demonstrated in *Figure 1.8*, access permissions are applied to an object based on the level of clearance given to a subject. The example provided represents only a few of the possible permissions that can be assigned to an object. For example, "list" is a permission seen in common operating systems that permits users to only list the files in a directory, not read, delete, modify, or execute those files.

Moreover, a single object can have multiple access permissions depending on the user or group that needs to access that object. As demonstrated in *Figure 1.9*, users can be assigned to groups, such as administrators or printer users. Anyone in the group administrators has full control over the user directories for Bruce, Sally, and Bob. However, users in the printer users group can only access local printers but not any of the user directories.

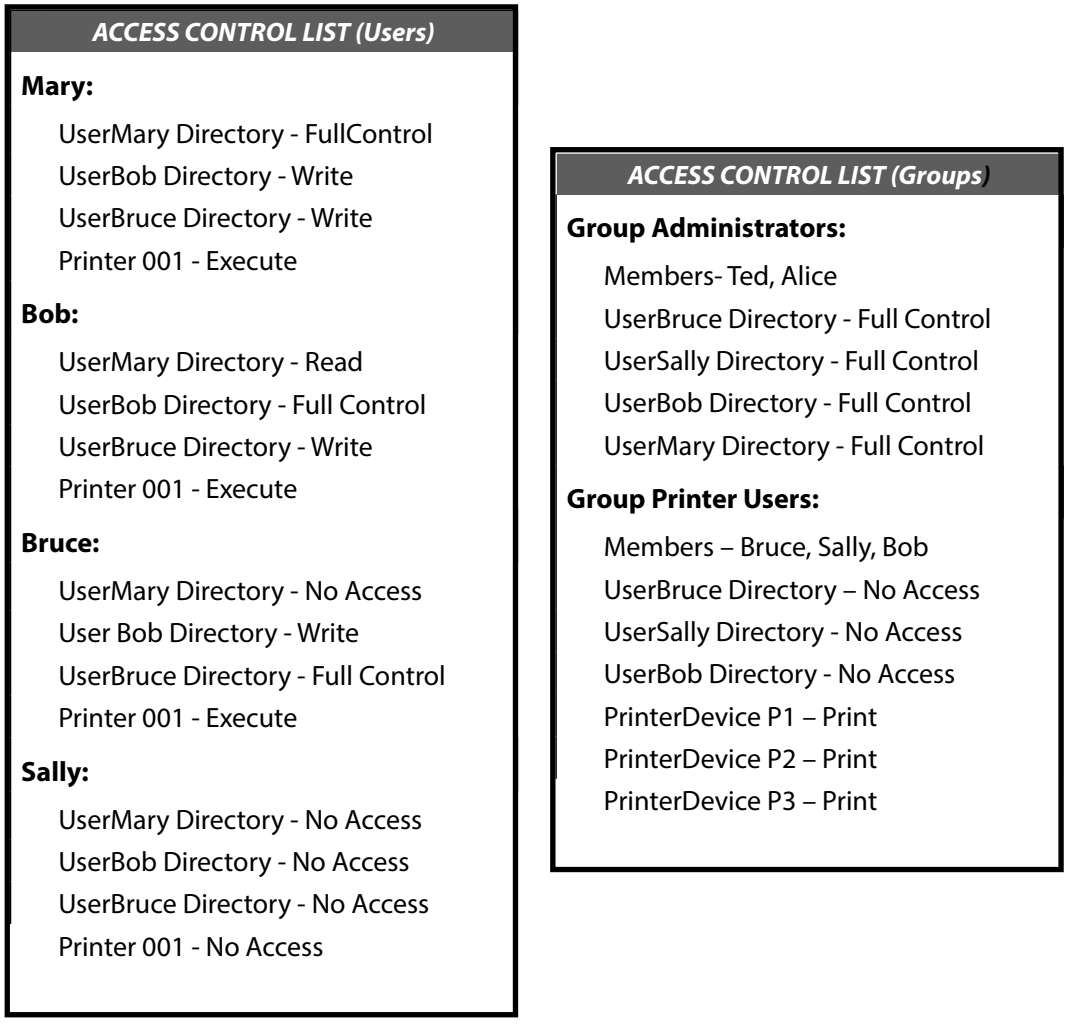


Figure 1.9 **- Access permissions and group roles. Users can be assigned to groups, such as Administrators or Printer Users. Anyone in the group Administrators has full control over the user directories for Bruce, Sally and Bob. However, users In the PrinterUsers group can only access local printers but not any of the user directories.**

The third access control framework, nondiscretionary access control, is also based on the assignment of permissions to read, write, and execute files on a system. However, unlike discretionary access control, which allows the file owner to specify those permissions, nondiscretionary access control requires the administrator of a system to define and tightly control the access rules for files in the system.

Data Access Controls

Data access controls can be implemented in a number of different ways depending on the access needs, organization requirements, and available technology capabilities. This section will discuss the more common methods of implementing effective data access control.

The term access control list (ACL) is used in many forms to communicate how a collection of controls is assigned based on a particular set of parameters. ACLs will typically have two basic pieces of data: a keyword pattern and an action to take if the keyword is matched. The pattern of the keyword will vary based on the application. For example, if the ACL is located in a network router the keyword will be an IP address or network designation and the action will consist of instructions on whether to block the traffic from (or to) that network or allow it to pass through. If the ACL is attached to a file on a server, the keyword will be a user ID or system group and the action will be an indication of whether that user or group will be allowed to access the requested file. There will be many such keyword/action pairs in an ACL and the system will continue searching down the list until it finds a match. If no match is found, all ACL systems include a default action (usually "block" or "permit"). That default action will be based primarily on the organization's overall security stance. In other words, whether it belongs to the "deny by default" or "allow by default" philosophy security will determine the ultimate fate of unspecified actions.

ACLs are often used in the provisioning of permissions within a system based on organization policy. In most cases, ACLs within a system are applied to actions by the user, but they can also be tied to group permission. For example, an administrator may create a set of users, assign them to a group, and apply a set of files and directory permissions to that group. Within the system that information is translated into an ACL that is then employed when access to that file or directory is requested.

Access Control Matrix

An access control matrix (ACM) is an ACL in the form of a table. Subjects and objects are identified and the permissions applied to each subject/object combination are specified in the matrix. As shown in *Figure 1.10*, an ACM can be used to quickly summarize what permissions a subject has for various system objects. This is a simple example, and in large environments an ACM can become quite complex. But, it can be extremely helpful during system or application design to ensure that security is applied properly to all subjects and objects throughout the application.

Subject	A	B	C	D	E	F	G	H	I	J	K	X
1	●			●								●
2						●				●		
3	●								●			
4					●			●				●
5		●										
6							●					
7			●						●			

Figure 1.10 - **An Access Control Matrix (ACM) is an ACL in the form of a table. Subjects and objects are identified and the permissions applied to each subject/object combination are specified in the matrix. Here, an ACM can be used to quickly summarize what permissions a subject has for various system objects. This is a simple example. In large environments an ACM can become quite complex.**

Rule-Based Access Control

In a rule-based system, access is based on a list of predefined rules that determine what accesses should be granted. The rules, created or authorized by system owners, specify the privileges granted to users (e.g., read, write, and execute) when the specific condition of a rule is met. For example, a standard ACL may specify simply that user Bob is allowed to access the file

labeled "Financial Forecast," but a rule-based system would additionally specify that Bob can only access that file between 9:00 AM and 5:00 PM Monday through Friday. A mediation mechanism enforces the rules to ensure only authorized access by intercepting every request, comparing it to user authorizations, and making a decision based on the appropriate rule. Rule-based controls are most commonly a form of DAC, because the system owner typically develops the rules based on organization or processing needs.

Role-Based Access Control

A role-based access control (RBAC) model, as shown in *Figure 1.11*, bases the access control authorizations on the roles (or functions) that the user is assigned within an organization. The determination of what roles have access to a resource can be governed by the owner of the data, as with DACs, or applied based on policy, as with MACs.

Access control decisions are based on job function, previously defined and governed by policy, and each role (job function) will have its own access capabilities. Objects associated with a role will inherit privileges assigned to that role. This is also true for groups of users, allowing administrators to simplify access control strategies by assigning users to groups and groups to roles.

There are several approaches to RBAC. As with many system controls, there are variations on how they can be applied within a computer system. As demonstrated in *Figure 1.11*, there are four basic RBAC architectures:

1. ***Non-RBAC***: Non-RBAC is simply a user-granted access to data or an application by traditional mapping, such as with ACLs. There are no formal "roles" associated with the mappings, other than any identified by the particular user.
2. ***Limited RBAC***: Limited RBAC is achieved when users are mapped to roles within a single application rather than through an organization-wide role structure. Users in a limited RBAC

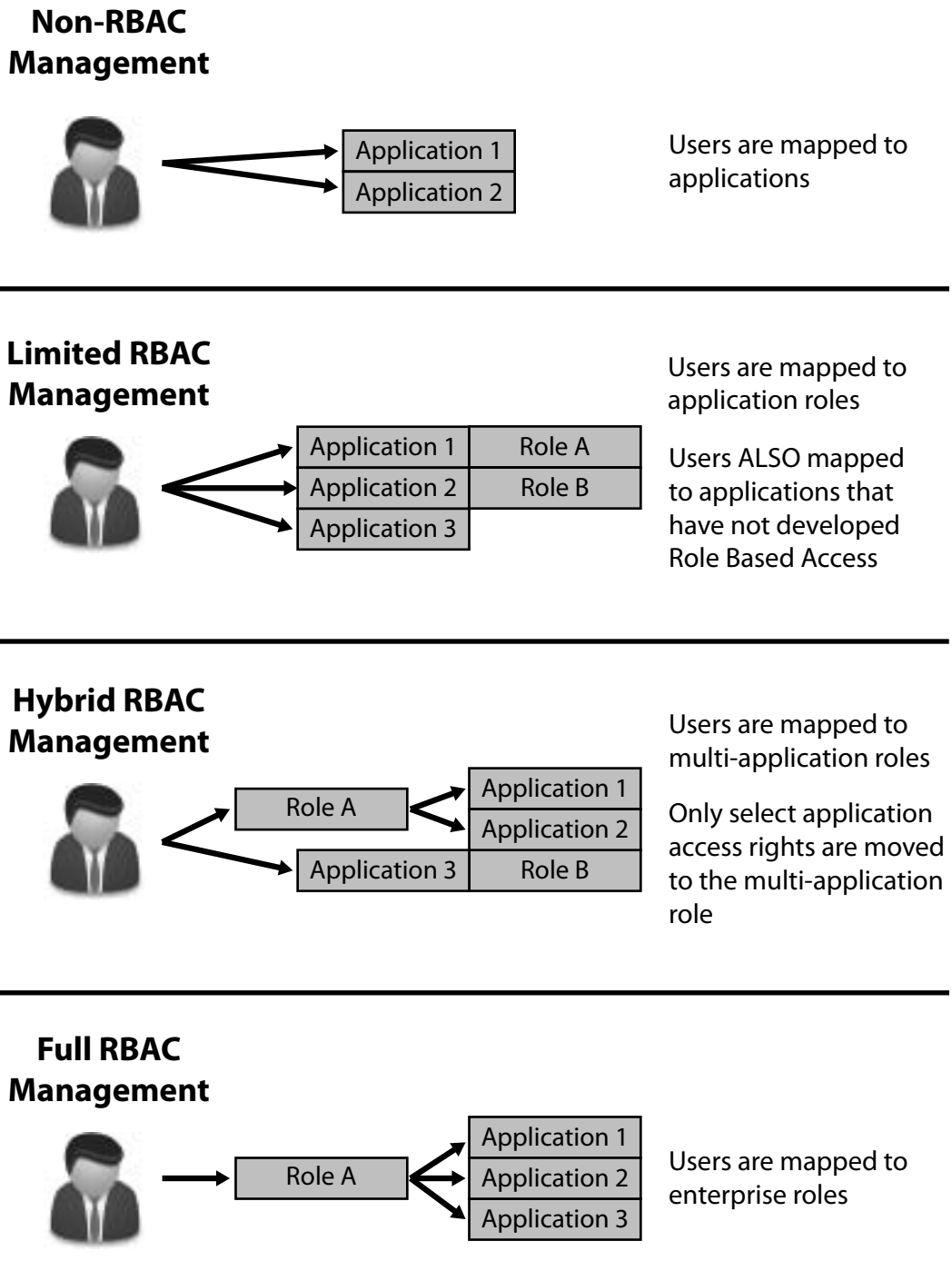


Figure 1.11 **- Role-Based Access Control architecture**

system are also able to access non-RBAC-based applications or data. For example, a user may be assigned to multiple roles within several applications and, in addition, have direct access to another application or system independent of his or her assigned role. The key attribute of limited RBAC is that the role for that user is defined within an application and not necessarily based on the user's organizational job function.

3. ***Hybrid RBAC***: Hybrid RBAC introduces the use of a role that is applied to multiple applications or systems based on a user's specific role within the organization. That role is then applied to applications or systems that subscribe to the organization's role-based model. However, as the term "hybrid" suggests, there are instances where the subject may also be assigned to roles defined solely within specific applications, complimenting (or, perhaps, contradicting) the larger, more encompassing organizational role used by other systems.
4. ***Full RBAC***: Full RBAC systems are controlled by roles defined by the organization's policy and access control infrastructure and then applied to applications and systems across the enterprise. The applications, systems, and associated data apply permissions based on that enterprise definition, and not one defined by a specific application or system.

The primary benefit of an RBAC-based access system is that it is easily modeled after the organization's own organization or functional structure. Just as employees have roles within the political hierarchy of the organization, so, too, do they have roles in the functional hierarchy of an information system. In addition, accounting for the movement of personnel around an organization and adjusting their information access accordingly is greatly simplified in an RBAC-based system. The administrator simply removes the old role designation from the user (instantly removing access to all information the old role required) and assigns that user to a new role, automatically granting that user access to all the information assigned to that new role.

Content-Dependent Access Control

Some access control decisions are affected by the actual content of the data rather than on overall organizational policy. For example, consider the typical payroll database where personnel from multiple levels require access. Managers should be able to view payroll information for their own staff but not for their peers or any other employees. This means that even though the user may be able to access the database in question, their ability to view the data within the database may be restricted according to the value of the data—in other words they may only be able to see records with the same department number as the department they belong to. The typical role-based functions may be applied to the database (e.g., manager, employee, administrator, etc.) but the logical structure of the data will be constantly changing.

Personnel move between departments, managers change assignments (and staff) and company reorganizations often mean that personnel can move from one division to another rapidly. In that type of environment the roles "manager" and "worker" may be valid, but the personnel that fall into those categories may change often over time. For that reason, some systems use content-dependent access control. Content-dependent access control is based on the actual content of the data rather than on general role definitions. It requires the access control mechanism (via an arbiter program within the software application or system used to access the data) to investigate the data to make decisions on how to apply the access rules in the system. With a content-dependent model the policy and access rules do not change, but the actual data a user may be able to see as a result of applying those changes may change over time as the data itself changes.

Constrained User Interface

Another method for controlling access is by restricting users to specific functions based on their role in the system. This is typically implemented by limiting available menus, data views, encryption, or by physically constraining the user interfaces. This is common on devices such as an

automated teller machine (ATM). In the previously mentioned payroll database example, someone in an "employee" role would only have options for "view paycheck" and "change tax info," whereas a manager using the same system might be give the additional options of "grant a raise" and "promote employee" (but not for himself, of course!) The advantage of a constrained user interface is that it limits potential avenues of attack and system failure by restricting the processing options that are available to the user. On an ATM machine, if a user does not have a checking account with the bank he or she will not be shown the "Withdraw money from checking" option. Likewise, an information system might have an "Add/Remove Users" menu option for administrators, but if a normal, non-administrative user logs in he or she will not even see that menu option. By not even identifying potential options for non-qualifying users, the system limits the potentially harmful execution of unauthorized system or application commands.

Many database management systems have the concept of "views." A database view is an extract of the data stored in the database that is filtered based on predefined user or system criteria. This permits multiple users to access the same database while only having the ability to access data they need (or are allowed to have) and not data for another user. The use of database views is another example of a constrained user interface.

Capability Tables

Capability tables are used to match subjects (like users or processes) and their capabilities (like read, write, and update) against system objects (like files, directories, and devices) and the ability to use those capabilities on those objects. *Figure 1.12* shows a good example of how this works.

Subject	Procedure A	File X	File Y
Process A		Read	Read/Write
Joe	Execute	Write	

Figure 1.12 - **A good example of how a capability table works.**

Each row in the table holds the capabilities for a specific subject (like a process or a user). Each column represents an object in the environment. As you move across the columns for a particular row you can see what capability each subject can apply to each particular object. For example, Process A (subject) has read-only access to File X and read/write capability to File Y. Joe, on the other hand, can execute Process A and write to File X but has no ability to access File Y.

Temporal (Time-Based) Isolation

There are often times when certain activities on a system are considered either acceptable or unacceptable based not on who performs those activities, but rather on when they are performed. Temporal or timed-based access controls are those employed at a given time for a predetermined duration. If a request is made for access to data or a resource outside the defined time window, the access is denied. For example, a bank may want its employees to only access its loan application system during business hours (when, presumably, they are in the office) and not at night or on the weekends (when they would be at home or elsewhere). Likewise, an organization could establish their information processing service such that only confidential data will be processed in the morning, when all their workers possessing a "Confidential" clearance are scheduled to work. All secret data will then be processed in the afternoon, when workers with a "Secret" clearance are on the schedule. Attempts to access confidential data in the afternoon or secret data in the morning would be denied.

This concept can also extend to system processing, where certain types of jobs may only be run during certain parts of the day or on certain days of the year. For example, a business would not want its end-of-month processing to be run in the middle of the month, so it may restrict access to that process such that it can only be run from the 1st to the 5th days of any month. There is one important caveat to using temporal access controls: if the organization is spread across several time zones care must be taken to ensure that the time differences between locations are accounted

for in both the process and the supporting technology. For example, if an organization defines "secret" access as being available only between 8:00 AM and 11:00 AM and has offices in both New York and Hong Kong the organization must define which location will serve as the reference point. Otherwise, it is possible that secret information will be accessible for a total of six hours (three in New York and three in Hong Kong) rather than the intended three

Identification and Authentication

To this point the chapter has focused on access control principles and the threats to the control environment. The section that follows covers details regarding specific access controls and essential control strategies. Areas include:

- Identification, authentication, and authorization
- Access control services
- Identity management
- Access control technologies

Identification, Authentication, and Authorization

Identification is the assertion of a unique identity for a person or system and is the starting point of all access control. Without proper identification it is impossible to determine to whom or what to apply the appropriate controls. Identification is a critical first step in applying access controls because all activities and controls are tied to the identity of a particular user or entity.

The downstream effects of proper identification include accountability (with a protected audit trail) and the ability to trace activities to individuals. They also include the provisioning of rights and privileges, system profiles, and availability of system information, applications, and services. The objective of identification is to bind a user to the appropriate controls based on that unique user instance. For example, once the unique user is identified and validated through authentication, his or her identity within the infrastructure will be used to allocate resources based on predefined privileges.

Authentication is the process of verifying the identity of the user. Upon requesting access and presenting unique user identification, the user will provide some set of private data that only the user should have access to or knowledge of. The combination of the identity and information only

known by, or only in the possession of, the user acts to verify that the user identity is being used by the expected and assigned entity (e.g., a person). This, then, establishes trust between the user and the system for the allocation of privileges.

Authorization is the final step in the process. Once a user has been identified and properly authenticated, the resources that user is allowed to access must be defined and monitored. Authorization is the process of defining the specific resources a user needs and determining the type of access to those resources the user may have. For example, Deanna, Jennifer, and Matthew may all be identified and authenticated into the same system, but Deanna is only authorized to access the payroll information, Jennifer is only authorized to access product source code, and Matthew is only authorized to view the company's internal Web sites.

The relationship between these three important concepts is simple:

- Identification provides uniqueness
- Authentication provides validity
- Authorization provides control

Identification Methods

The most common form of identification is a simple user name, user ID, account number, or personal identification number (PIN). These are used as a point of assignment and association to a user entity within a system. However, identification may not be limited to human users and may include software and hardware services that may need to access objects, modules, databases, or other applications to provide a full suite of services. In an effort to ensure that the application is authorized to make the requests to potentially sensitive resources, the system can use digital identification, such as a certificate or one-time session identifier to identify the application. There are several common forms of identification used by organizations, and the type used may vary depending on the process or the situation.

Identification Badges

An identification badge is the most common form of physical identification and authorization in organizations. The badge represents that the badge holder is officially recognized and has some status within the organization. Most badges contain the name or logo of the organization, the name of the badge holder, and a picture of the holder printed on the face. In some cases, because of the cost of badge printing, organizations will print personalized badges only for employees. Visitors or temporary personnel will be given a generic badge, perhaps in a different color, to signify that they are permitted on the premises but do not belong to the organization.

The typical process behind an ID badge requires that the user wear the badge at all times while on company premises. Employees and security personnel will be able to observe the badge, check the picture on the badge against the badge wearer, and then make a determination as to whether the person legitimately belongs on the premises or not. If the name, picture, and badge holder do not all match, the employee should summon security or escort the badge holder off the premises.

Unfortunately, this process fails all too often. Most people, even security guards, fail to make a very close comparison of the badge against the holder. During the morning rush into a facility most employees simply wave the badge in the air to indicate they have one and are allowed to pass. While this is not a universal problem—government and military facilities generally pay close attention to badge holders and their credentials—it is common enough to conclude that identification badges are not a foolproof security mechanism.

Another type of badge, the access badge, provides a much stronger security mechanism. Access badges are used to enter secured areas of a facility and are used in conjunction with a badge reader to read information stored on the badge. A central monitoring facility will read the badge information, match that information against a list of authorized personnel for that area,

and make a determination for or against access. A failing of access badges is that, because they are not physically tied with a specific person, employees often share their badges with others who may need temporary access to a secured area. While certainly not endorsed by the organization, and most often directly counter to security policy, this practice is widespread. To counter this problem, many organizations combine the identification badge with the access badge to provide a stronger tie between the badge holder and the individual ID card.

User ID

The common user ID—the standard entry point to most information systems—provides the system with a way of uniquely identifying a particular user amongst all the users of that system. No two users on a single system can have the same user ID, as that would cause confusion for the access control system and remove the ability to track any activity to an individual. It is important to note that the user ID should only be used as a system identifier, not an authenticator. The user ID simply tells the system that this user wants to be identified by that ID, not that this user has the legitimate right to access the system under that ID or be given access to any system resources. It is only when the user ID is combined with some other authentication mechanism, such as a password, security token, or a digital certificate, that a judgment can be made as to the legitimacy of the user and access can be permitted or denied.

Account Number/PIN

Much like a user ID, an account number provides a unique identity for a particular user within a system or an enterprise. Most ordinary users will encounter account numbers as part of a financial services application or transaction. In such transactions, the personal identification number (PIN), provides the authentication information needed to determine whether the user has the legitimate right to use that account number and access the information under that account.

MAC Address

All computers that participate in a network must have some method of uniquely identifying themselves to that network so that information can be sent to and from the network connection associated with the proper computer. The most common form of machine address in use today is the media access control (MAC) address. The MAC address is a 48-bit number (typically represented in hexadecimal format) that is supposed to be globally unique, meaning that every network device in the world is supposed to have a unique MAC address. In the early days of network computing, the MAC address was embedded into the hardware of the device during its manufacture and was not changeable by end users (or attackers). When that was the case, the MAC address was a good way to identify (and authenticate) particular devices with a high degree of certainty. Unfortunately, most modern network-enabled devices allow the MAC address to be set in software, meaning that anyone with administrative access to the device can alter the MAC address of that device to anything of his choosing. Thus, the MAC address is no longer considered a strong identifier or authenticator.

IP Address

Computers using the TCP/IP network protocol are also assigned an internet protocol (IP) address. Whereas the MAC address provides a way of identifying the physical location of a system, the IP address gives the logical location of a device on the IP network. IP addresses are organized into logical groups called subnetworks or subnets. A device's IP address must be unique among all the systems on that device's same subnet, but there are circumstances where devices on different subnets can have identical IP addresses. As was the case with MAC addresses, a device's IP address is assigned in software by the administrator of a system. As such, IP address is not a very strong indicator of a system's identity. It is possible to use the IP address as one data point amongst many to narrow down a system's unique network location or identity, but it should not be used alone for such purposes.

Radio Frequency Identification (RFID)

In recent years, a great deal of research has been done to determine ways to uniquely identify objects and be able to read that identification without physically interacting with the object itself. This can be very useful in cases where it is advantageous to identify items quickly or without the need for physical inspection. The most popular technology to come out of this research is the radio frequency identification (RFID), tag. The RFID tag is a small label that can be embedded in almost any object, including product shipping pallets, passports, consumer goods, and even human beings. The tag contains identifying information for the object, such as a UPC code or a person's name. When the tag comes in the proximity of an RFID reader, the reader reads the information from the tag and determines the identity of the object. RFID tags are extremely small, so they add no discernible size or weight to the object being tagged, and because they can be read from a distance of several feet the reader does not need close physical contact with the tagged object.

The use of RFID in some applications has raised some privacy concerns for some people. For instance, RFID tags are now included in all newly issued passports for several countries such as the U.S. and Australia. Unfortunately, because the tags can be read from a distance, many fear that their private passport information can be taken from the tag without their consent. In addition, many are advocating the injection of RFID tags into humans to allow authorities to positively identify those people if they are kidnapped or killed. Again, privacy advocates fear that RFID-injected people can have their personal tag information read without their consent by an intruder with a tag reader in a crowded public place, raising identity theft concerns. In the final analysis, RFID technology has been a big breakthrough in the manufacturing and consumer goods industries where it is helping to reduce inventory and product tracking costs. The values and risks to privacy and breach must be considered when using an RFID badge.

E-Mail Address

The use of a person's e-mail address as an identification mechanism or user ID has become increasingly popular in recent years, particularly for Internet e-commerce and portal sites. Part of the reason for this is that an e-mail address is globally unique. If a user's e-mail address is janet@jmail.com, nobody else can legitimately use that address to send or receive e-mail. Based on that assumption, many Web sites use the user's e-mail address as the unique user ID and allow the user to select a password for authentication. Web sites using this convention will additionally use that e-mail address to send correspondence to the user for administrative or informational purposes. One common mechanism in current use is to have a new user to register on the site to enter his e-mail address as a user ID. The site will then send a confirmation e-mail to that address and wait for a reply from the user before completing the registration process. The theory behind this process is that if a user has access to the e-mail account specified by the entered address there is a high degree of certainty that the user is legitimate.

However, this assumption may not be valid in many situations. The uniqueness of an e-mail address is enforced solely by convention. There are no technical restrictions preventing the use of another person's e-mail address as an identifier and, the aforementioned verification mechanism notwithstanding, there is no way to formally verify the legitimacy of a particular e-mail address or that a particular individual is the owner of that address. In addition, it is a simple matter to spoof (or falsify) the sender's e-mail address in most common e-mail systems in use today, and spammers, fraudsters, and phishing perpetrators regularly use this method as a way of masking the true origin of their attacks. It is convenient for a person to use an e-mail address as identification because it is easy to remember, but if an organization wishes to use this as an identification method it should not place absolute trust in its legitimacy and should certainly use other authentication methods to tie the use of that address to a particular user.

User Identification Guidelines

There are three essential security characteristics regarding identities: uniqueness, nondescriptiveness, and secure issuance. First and foremost, user identification must be unique so that each entity on a system can be unambiguously identified. Although it is possible for a user to have many unique identifiers, each must be distinctive within an access control environment. In the event there are several disparate access control environments that do not interact, share information, or provide access to the same resources, duplication is possible. For example, a user's ID at work may be "mary_t," allowing her to be identified and authenticated within the corporate infrastructure. She may also have a personal e-mail account with her Internet service provider (ISP) with the user ID of "mary_t." This is possible because the corporate access control environment does not interact with the ISP's access control environment. However, there are potential dangers with using the same ID on multiple systems. Users are prone to duplicating certain attributes, such as passwords, to minimize their effort. If an attacker discovers Mary's ISP ID and password, he or she may rightly conclude that she is using the same ID and password at work. Therefore, any duplication, although possible in certain circumstances, represents a fundamental risk to the enterprise.

User identification should generally be nondescriptive and should try as much as possible to disclose as little as possible about the user. The ID should also not expose the associated role or job function of the user. Common practice is to issue user IDs that are a variant of the user's name, for example, "bsmith" or "bob.smith." Once this scheme is identified by an attacker it becomes easy to begin enumerating through possible variations on the theme to discover other valid user IDs in the organization. In addition, a person's job function should never be used as the basis for a user ID. If a user ID were to be named "cfo," an attacker would be able to focus energy on that user alone based on the assumption that he is the CFO of the company and would probably have privileged access to critical systems. However, this is practiced quite often. It is very common

to have user IDs of "admin," "finance," "shipment," "Web master," or other representations of highly descriptive IDs. The naming of these IDs is voluntary and self-imposed by the organization.

There are some IDs, however, that cannot be easily changed. The most predominant is the username "root." It is the name given to the administrative account with unlimited access rights on a UNIX system. Everyone, including attackers, knows what the username "root" represents, and it is for this very reason that attaining root's password is so desirable. Unfortunately, in most UNIX systems, changing the user or masking that role is impossible. In Microsoft operating systems it is possible to change the username of the default "administrator" account (nearly the equivalent of "root" in UNIX) to some other nondescriptive name, and should be considered a best practice.

Clearly, any highly privileged system account, such as "root" and "administrator," represents a target for attackers, and it can be difficult to mask its role. However, traditional users, who may have a broad set of privileges throughout the enterprise, can be more difficult for attackers to isolate as a target. Therefore, establishing a user ID that is independent of the user's name, job function, or role will act to mask the true privileges of the user. Ideally, user IDs should be randomly assigned or include some randomized elements to prevent ID guessing and enumeration by attackers. While renaming is a best practice and will prevent rudimentary attempts at access it can be defeated by identifying the "Security IDs." Defense in depth must be practiced to ensure an appropriate level of defense is implemented vs. the burden to the user and risk.

Clearly, any highly privileged system account, such as "root" and "administrator," represents a target for attackers, and it can be difficult to mask its role. However, traditional users, who may have a broad set of privileges throughout the enterprise, can be more difficult for attackers to isolate as a target. Therefore, establishing a user ID that is independent of

the user's name, job function, or role will act to mask the true privileges of the user. Ideally, user IDs should be randomly assigned or include some randomized elements to prevent ID guessing and enumeration by attackers.

Finally, the process of issuing identifiers must be secure and well documented. The quality of the identifier is in part based on the quality of how it is issued. If an identity can be inappropriately issued, the entire security system can break down. The identifier is the first, and arguably the most important, step in acquiring access. An organization must establish a secure process for issuing IDs, including the proper documentation and approval for all ID requests. The process must also account for notification of the user's management and any system owners for systems the user may have access to. The organization must deliver the user ID to the end user in a secure manner. This can be as simple as delivery in a sealed envelope or as complicated as using digitally signed and encrypted communications channels. Finally, the entire process must be logged and documented properly to ensure that the process can be verified and audited.

Identity Management

Identity management is a much-used term that refers to a set of technologies intended to offer greater efficiency in the management of a diverse user and technical environment. Modern enterprises must deal with the difficulties of managing the identity and access restrictions of employees, contractors, customers, partners, and vendors in a highly complex and dynamic organization. Identity management systems are designed to centralize and streamline the management of user identity, authentication, and authorization data.

Identity management addresses all aspects of controlling access, with a core focus on centralized management. Given the complexity of modern organizations and the diversity of business requirements, many access control infrastructures grow convoluted and difficult to manage. They

manage multiple independent access control systems, often one per application. Rarely are they all integrated; at best there may be pockets of integration between several applications. Along with this multiplicity of access control systems comes a complex web of administrative responsibilities, making the administrator's job even more complex with each new application. Enterprises operate a vast array of IT infrastructure components, including:

- Network operating systems
- Multiple servers running multiple operating systems
- User directories
- Human resources, payroll, and contract management systems
- A variety of line-of-business applications
- Customer relationship management (CRM) systems
- Electronic commerce applications
- Enterprise resource management systems planning (ERP)

As shown in *Figure 1.13*, almost every system must track valid users and control their permissions for a given system. The diversity of these systems—each with its own administration software, and management processes—and the fact that users typically access multiple systems, makes managing this user data difficult at best, and a financial and operational burden to most organizations.

One of the primary tasks within an identity management infrastructure is the need to provision, maintain, and manage user IDs. This includes gathering the initial account information to populate the system and create an account record for that user. The information may be submitted by the user through filling out a standard form or an in-person interview, or it may come directly from the user as part of a self-help service. Once account information is gathered, the system must be able to account for the granting and revocation of access rights as the user (and the associated IDs) goes through its natural life cycle.

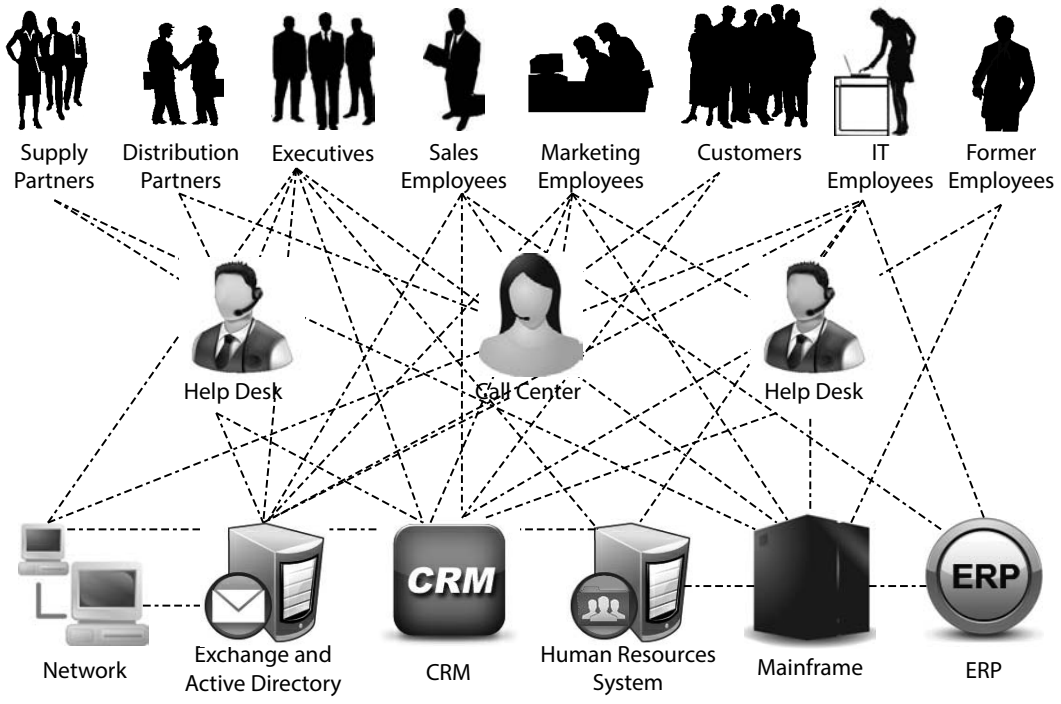


Figure 1.13 - **In complex environments, almost every system must track valid users and control their permissions.**

Efficiency in this process is a key performance factor. The goal of an identity management system is to consolidate access rights into an easily managed record of identity and access for each user in the system. This will work to reduce errors and increase control over IDs and access in the organization. It will also eliminate redundant and unnecessary access. "Once and done" is the mantra for this activity. Setting up user access on multiple systems is repetitive. Doing so with the individual tools provided with each system is needlessly costly. Therefore, all design and development for the identity management system should be aimed at reducing redundancy and streamlining the provisioning and management processes as much as possible.

Timeliness of the process is important to the business. If there is too much of a time lag during the front-end provisioning and management processes, that will translate directly to lost user productivity. If there is a time lag

during the access removal or decommissioning stages, that will translate into increased security risk to the organization. Identity management systems promote timeliness by centrally managing the identity and access control for distributed systems throughout the enterprise.

Identity Management Challenges

Typically, when an employee is hired, a new user profile is created and stored in a human resources database and a request for access to various systems and applications is created. If the organization has predefined roles associated with particular jobs the new user request will be compared to a company's role authorization policies. If the organization does not have such a role-based system, a management-defined list of access rights will be created. The request is then routed for the necessary approval, and (if approval is granted) sent to the IT department. Finally, the IT department submits the approved request to various system administrators to provision user access rights. The user is provisioned, and the approval is recorded in a history file or log file.

This scenario assumes, of course, the best of all possible worlds, where processes work perfectly every time and all participants are prepared to do their part at any time. In actual practice, there are a number of problems that can arise during the identity management process:

- Requests for access rights can be backlogged, halting user productivity. There will be a limited number of people to process these requests and often this is not an individual's (or a group's) full-time job. As a result, these requests are often delayed or held until enough requests are pending for someone to allocate time to process them.
- Cumbersome policies cause errors. If the requested access involves different systems and complex levels of access there is a high likelihood that there will be errors in the implementation of the request. This will result in delayed access (at best) or the assignment of inappropriate access to the user (at worst).
- Request forms are not fully completed. This can cause

numerous delays in processing. Very often, the forms are not clear or the requestor is confused as to specifically what they need to request.

- The number of resources across the enterprise may be growing. This may lead to an increasing number of access requests continually flowing into the processing system. Given the chronic resource shortage in most organizations, this will become a perpetual problem.
- Precise audit trails of requests and approvals are rarely maintained. If there is a question about what access was requested, who approved it, or what was ultimately granted, an audit trail is the only definitive method of determining this. Unfortunately, many organizations do not keep accurate records of this process, particularly during the approval stages.
- Many system profiles and users are dormant or associated with departed employees, making them invalid. The process of removing access when no longer needed is just as important as granting it in the first place. However, many organizations fail to implement processes to regularly review existing access to determine if it is still needed.

Some people in the organization, particularly those in the upper levels of management, often bypass defined processes and protocols put in place to manage the flow of provisioning requests in an attempt to get their requests implemented more quickly. Even employees at lower levels in the organization may attempt to call a helpful friend in IT rather than go through the standard process. If allowed to continue, this practice leads to inaccurate record keeping as some provisioning will not be properly recorded.

Key management challenges regarding identity management solutions also include:

- ***Consistency:*** User profile data entered into different systems should be consistent. This includes name, user ID, contact