Security Workbook

December 20, 2023 - Version 8

Author: Susan Lincke PhD CISA CRISC

lincke@uwp.edu

This workbook is designed to assist small-medium organizations in developing a mature IT framework: to increase reliability, security, confidentiality and reduce risk relating to the IT area and the organization as a whole. It can be applied to not-for-profit, for-profit, or government organizations, and may serve as a starting point for larger organizations. The workbook creates a foundation to adhere to security regulation commonly required by such businesses, but may not address legislation applicable to a specific industry.

Security Workbook

[1. Introduction 6](#_Toc155712286)

[1.1 Overview 7](#_Toc155712287)

[1.1.1 Planning Tactical Security: Addressing Specific Security Areas 8](#_Toc155712288)

[1.1.2 Planning Audit 8](#_Toc155712289)

[1.2 Permissions 10](#_Toc155712290)

[1.3 Recognition of Contribution 10](#_Toc155712291)

[2. Strategic Security Planning 10](#_Toc155712292)

[2.1 Identifying Security Issues and Legal Compliance 10](#_Toc155712293)

[2.1.1 Identify Threat agents and Cyber Threats 10](#_Toc155712294)

[2.1.2 Identify Fraud Threats 11](#_Toc155712295)

[2.1.3 Identify Social Engineering Threats 12](#_Toc155712296)

[2.1.4 Identify Applicable Regulation/Standards 12](#_Toc155712297)

[2.2 Managing Risk 15](#_Toc155712298)

[2.2.1 Step 1: Determine Value of Assets (Crown Jewels): 15](#_Toc155712299)

[2.2.2 Step 2: Estimate Potential Loss for Threats: 17](#_Toc155712300)

[2.2.3 Step 3: Estimate Likelihood of Exploitation 18](#_Toc155712301)

[2.2.4 Step 4: Compute Expected Loss 19](#_Toc155712302)

[2.2.5 Step 5: Treat Risk 19](#_Toc155712303)

[2.2.6 Advanced: Deciding on Risk Tolerance: 21](#_Toc155712304)

[2.3 Addressing Business Impact Analysis & Business Continuity 22](#_Toc155712305)

[2.3.1 Business Impact Analysis 22](#_Toc155712306)

[2.3.2 Step 3: Plan for Recovery (Business Continuity) 25](#_Toc155712307)

[2.4 Governing with a Policy Manual 28](#_Toc155712308)

[2.4.1 IT Strategic Planning 28](#_Toc155712309)

[2.4.2 Security Management 29](#_Toc155712310)

[2.4.3 Information Asset Protection 29](#_Toc155712311)

[2.4.4 Risk Management 29](#_Toc155712312)

[2.4.5 Access Control 29](#_Toc155712313)

[2.4.6 System Security 30](#_Toc155712314)

[2.4.7 Human Resources 30](#_Toc155712315)

[2.4.8 Business Continuity 30](#_Toc155712316)

[2.4.9 Physical Controls 31](#_Toc155712317)

[2.4.10 Change Management 31](#_Toc155712318)

[2.4.11 Internal Control 31](#_Toc155712319)

[2.4.12 Software/Hardware/Service Acquisition & Management 31](#_Toc155712320)

[2.4.13 Third Party Services 32](#_Toc155712321)

[2.4.14 IT-IS Management 32](#_Toc155712322)

[2.4.15 Process Improvement 32](#_Toc155712323)

[2.4.16 Legal and Contractual Obligations 32](#_Toc155712324)

[2.5 Preparing a Code of Ethics 33](#_Toc155712325)

[3. Tactical Security Planning 34](#_Toc155712326)

[3.1 Designing Information Security 34](#_Toc155712327)

[3.1.1 Step 1: Classify Data for CIA 35](#_Toc155712328)

[3.1.2 Step 2: Allocate Controls 37](#_Toc155712329)

[3.1.3 Step 3: Allocate Roles and Permissions 38](#_Toc155712330)

[3.2 Planning for Network Security 40](#_Toc155712331)

[3.2.1 Step 1: Determine Services and Devices which may Enter and Leave the Network 40](#_Toc155712332)

[3.2.2 Step 2: Determine Sensitivity of Services 41](#_Toc155712333)

[3.2.3 Step 3: Allocate Network Zones 42](#_Toc155712334)

[3.2.4 Step 4: Define Controls 43](#_Toc155712335)

[3.2.5 Step 5: Draw the Network Diagram 45](#_Toc155712336)

[3.3 Designing Physical Security 46](#_Toc155712337)

[3.3.1 Step 1: Inventory Assets within Rooms 46](#_Toc155712338)

[3.3.2 Step 2: Selecting Controls for Sensitivity Classes 46](#_Toc155712339)

[3.3.3 Step 3: Selecting Controls for Criticality Classes 47](#_Toc155712340)

[3.3.4 Step 4: Complete the Physical Security Map 48](#_Toc155712341)

[3.4 Attending to Information Privacy 49](#_Toc155712342)

[3.4.1 Step 1: Defining a Data Dictionary with Primary Purpose 49](#_Toc155712343)

[3.4.2 Step 2: Performing a Privacy Impact Assessment 49](#_Toc155712344)

[3.4.3 Step 3: Developing a Policy and Notice of Privacy Practices 51](#_Toc155712345)

[3.5 Managing Cloud Security 53](#_Toc155712346)

[3.5.1 Step 1: Define Security and Compliance Requirements 53](#_Toc155712347)

[3.5.2 Step 2: Select a Cloud Provider and Service/Deployment Model 54](#_Toc155712348)

[3.5.3 Step 3: Define architecture 56](#_Toc155712349)

[3.5.4 Step 4: Assess shared security responsibility: your’s & cloud’s 56](#_Toc155712350)

[3.5.5 Step 5: Monitor and manage changes 57](#_Toc155712351)

[3.6 Organizing Personnel Security 58](#_Toc155712352)

[3.6.1 Step 1: Controlling Employee Threats 58](#_Toc155712353)

[3.6.2 Step 2: Allocating Responsibility to Roles 60](#_Toc155712354)

[3.6.3 Step 3: Define Training, Documentation and Tools to Manage Security 61](#_Toc155712355)

[3.7 Planning for Incident Response 62](#_Toc155712356)

[3.7.1 Step 1A: Determine types of concerning attacks and how they will be detected 62](#_Toc155712357)

[3.7.2 Step 1B: Design the Incident Response Handling Forms 65](#_Toc155712358)

[3.8 Defining Security Metrics 67](#_Toc155712359)

[3.8.1 Approach 1: Implementing Business-Driven Metrics 67](#_Toc155712360)

[3.8.2 Approach 2: Implementing Technology-Driven Metrics 69](#_Toc155712361)

[3.9 Planning to Gather Forensic Information 70](#_Toc155712362)

[3.9.1 Aspect 1 Forensic Analysis: Establishing Forensic Questions 70](#_Toc155712363)

[3.9.2 Aspect 2 Technical Perspective: Methods to Collect Evidence 71](#_Toc155712364)

[3.9.3 Aspect 3 Legal Forensics: Ensuring Chain-of-Custody 71](#_Toc155712365)

[4. Performing an Audit 73](#_Toc155712366)

[4.1 Audit Planning 73](#_Toc155712367)

[4.2 Audit Engagement Plan Standard 74](#_Toc155712368)

[4.3 Evaluation of Design of Security Controls 74](#_Toc155712369)

[4.4 Audit Report Standard 75](#_Toc155712370)

[4.5 Audit Help Guides 77](#_Toc155712371)

[4.5.1 Equipment Baseline Audit 77](#_Toc155712372)

[4.5.2 Audit Questions for Employee Policy Adherence 78](#_Toc155712373)

[5. Operational Security Plans 79](#_Toc155712374)

[5.1 Information Security 80](#_Toc155712375)

[5.1.1 Information Security Standards 80](#_Toc155712376)

[5.1.2 Procedure for Authentication 81](#_Toc155712377)

[5.2 Computer & Server Security 82](#_Toc155712378)

[5.2.1 Computer/Server Security Standard 82](#_Toc155712379)

[5.2.2 Workstation/Laptop Security Configurations 83](#_Toc155712380)

[5.2.3 Procedures for Change Management 83](#_Toc155712381)

[5.2.4 Standards or Procedures for Software Installation 84](#_Toc155712382)

[5.3 Network Security 85](#_Toc155712383)

[5.3.1 Network Security Standard 85](#_Toc155712384)

[5.3.2 Router/Firewall Configurations 86](#_Toc155712385)

[5.4 Physical Security 87](#_Toc155712386)

[5.4.1 Physical Security Standard 87](#_Toc155712387)

[5.4.2 Physical Equipment Inventory 87](#_Toc155712388)

[5.5 Business Continuity 88](#_Toc155712389)

[5.5.1 Business Continuity Standard 88](#_Toc155712390)

[5.5.2 Procedures for Backup and Restore 88](#_Toc155712391)

[5.5.3 Procedures for Business Continuity 89](#_Toc155712392)

[5.5.4 Procedures for Incident Response 90](#_Toc155712393)

[5.5.5 Procedures for Disaster Recovery 90](#_Toc155712394)

[5.6 Personnel Security 91](#_Toc155712395)

[5.6.1 Personnel Security Standard 91](#_Toc155712396)

[5.6.2 Computer Use Training and Agreement 92](#_Toc155712397)

[5.6.3 Employee Hiring Standard 93](#_Toc155712398)

[6. References 94](#_Toc155712399)

[Appendix A: Incident Response Report 94](#_Toc155712400)

[Appendix B: IT Governance & Planning 96](#_Toc155712401)

# Introduction

This workbook is designed to assist small organizations to develop a mature IT framework, to increase reliability, security, confidentiality and reduce risk relating to the IT area and the organization as a whole. Threats to small companies arise from many sources. Internet exposure can increase organizational visibility and success, but exposes a computer network to attackers worldwide. Fraud reduces large companies’ income by an average of 5% annually[[1]](#endnote-2). However, fraud can devastate smaller organizations, which take longer to discover the fraud case and tend to lose larger sums of money. Computers and their networks will always fail at some time, and the organization must be prepared for such an occurrence. Finally, most businesses must adhere to one or more sets of legislation or standards. This book will help organizations to mature their IT and organizational security, to reduce risk, address common legislation, and to handle emergency events better.

Small businesses are commonly defined to be organizations with up to 500 employees. In our experience with community-based projects, many of these organizations have no full time information technology (IT) staff, or if they do, they have no full-time information security staff. The IT personnel they do employ have insufficient time and funds to address security needs, and they may also lack sufficient security training. This is a major problem since small businesses comprise 50% of the American Gross National Product and create 50% of all new jobs[[2]](#endnote-3). With such little security in place, NIST reports that criminals now find that smaller organizations are much easier to attack than the better funded, larger companies2.

However, while small businesses do lack security knowledge and implementation, they do have a couple of advantages over larger companies: the relationship between management and IT staff is closer in general. Communications is less compartmentalized. Management tends to have a better understanding and control over their operations, and this communication and control can help tremendously during the security development process. It is crucial during the security design process that management and IT work together to design security, and this workbook can serve as that framework.

This workbook is based on ISACA’s COBIT[[3]](#endnote-4), NISTIR 7621, as well as other professional security guides (CISA[[4]](#endnote-5), CISM[[5]](#endnote-6)) including some legislative standards. NISTIR 76212, entitled “Small Business Information Security: The Fundamentals”, is a publication of the American National Institute of Standards and Technology (NIST). COBIT is a maturity model developed for corporations who must address Sarbanes-Oxley legislation. Smaller organizations often do not have the manpower, structure, or need for the full COBIT model. This workbook can be applied to not-for-profit, for-profit, or government organizations, but may not address specific legislation applicable to an industry. For medium-sized organizations or other organizations very prone to security legislation (such as financial companies), this workbook can be used as a starting point to address security. The workbook provides direction for security design, but will require professional IT assistance for implementation. Note that a design without implementation is equivalent to no design at all.

Finally, security in general and this Workbook specifically is still a work-in-progress. Further iterations of the document will be more fully vetted. This Workbook provides no warantees for your security. However, not doing the workbook or some equivalent plan will virtually guarantee you to be hacked sometime by professional hackers.

THE MATERIAL IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL PUBLISHER OR AUTHOR BE LIABLE FOR ANY CLAIM, OR ANY DIRECT, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THESE MATERIALS.

This workbook has chapters listing specific recommended practices, and work pages with questions that the organization may address to its own needs. The book is best used in digital form, so that the organization can directly edit this workbook, post sections for employee viewing, and maintain standards as their business changes and grows. Organizations may choose to rename and divide the book to better address or disseminate its information.

## Overview

Responsibility can be divided between decision-making, or management functions, technical planning, operational procedures, and audit or compliance. This workbook addresses the four areas in separate chapters.

Management areas require decisions to be made at the top (or highest) management level, which provide direction based on business needs. Specific Strategic areas to be addressed are included in Chapter 2:

**Definition of Specific Threats**: The first area to focus on is what specific threats an organization is prone to. Threats or areas to consider include cybersecurity, fraud, social engineering and regulatory compliance. Background information is provided in Chapters 1-3 of *Information Security Planning: A Practical Approach.*

**Code of Ethics**: An organization must define what its employees, volunteers, and contractors can and cannot do. The Code of Ethics helps to prevent fraud and should be made available to personnel.

**Risk Analysis**: What risks could cause substantial damage to the organization? This section evaluates, documents, and addresses such risk.

**Business Impact Analysis**: If a computer server or network goes out-of-service, how would the organization cope? Which business functions cannot be manually done in an emergency? Data would be lost if a disk failure occurred: for how long (or for what duration) can the organization afford to lose data?

**Legal Compliance**: Which legislation must this organization pay attention to? This section looks at various regulations in the United States and how they affect various Small to Medium Enterprise (SME) industries, related to information security. It then indicates which sections of the workbook are applicable to each.

**Policy Manual**: A suggested set of policies for the IT department is provided. Policies applying to business functional areas should also be addressed. Once policies are defined, specific procedures or standards should be developed to ensure conformity.

### Planning Tactical Security: Addressing Specific Security Areas

Tactical areas of security address specific topics, and are appropriate for lower level management. For SME management and organizations that are new to security, this is a good place to start. A description of each with a case study example is provided in the text: *Information Security Planning: A Practical Approach.* Tactical security part of the workbook is included in Chapter 3, and defines the security architecture:

**Information Security**: Which data is of strategic or critical importance? Which data must remain confidential for legal, liability, business competition, trade secret, goodwill or reputational reasons? Data must be categorized and procedures must be defined for how each category of data is to be handled. Secondly, who should have access to confidential or critical data? How is authorization to be handled to ensure access is limited?

**Network Security**: Diagram the network to ensure adequate controls are in place. Technological controls (routers, firewalls), logical paths of entry (Internet, dial-up, wireless), and application servers are diagrammed to ensure Defense in Depth is provided.

**Physical Security**: Site(s) are diagramed to ensure adequate security. Physical controls include access controls: walls, locks, guards, and availability controls: air conditioning, UPS, fire suppressant systems. Rooms are categorized according to the class of data they contain.

**Incident Response**: If an attacker does enter the organization’s computer network, how should IT respond: close down the system immediately or continue operation? Should law enforcement be called in? When should management be notified? A list of actions to be immediately taken under various incident conditions is defined.

**Personnel Security**: Separation of Duties, if possible, helps to prevent fraud. Also, people need to be assigned security roles and trained to perform them.

**Metrics**: Metrics ensure that compliance to policies and security control is effective. This is a scorecard of the security program.

Specific business may need to address advanced areas, including:

**Information Privacy**: Required in European Union; aspects required in California. This evaluates how your customers may be impacted if their information is exposed.

**Cloud**: Giving your information over to another organization can save money and provide needed expertise and help, but lead to contractual issues such as information ownership, security, privacy, availability and backup, end-of-contract migration and (data) end-of-life.

**Forensics**: When an attack does occur, it is helpful to have the tools and/or help necessary to step in and analyze what occurred. This chapter outlines what information may be accessible where. However, advanced knowledge beyond this workbook is required.

### Planning Audit

This workbook provides audit standards as well, to help small organizations perform internal audits. Audit standards are listed in Chapter 4.

**Audit Planning Process**: Which are your most critical areas to be secured? Risk-based auditing considers these areas first.

**Audit Plan Standard**: Shows a format for an audit plan.

**Audit Report Standard**: Shows a format for an audit report.

**Equipment Baseline Audit:** This standardized form is used to audit a computer PC or workstation.

Chapter 5 includes the lowest level security documentation, including the Contextual and Operational levels. These levels define the required configurations of the security or secured devices, and the procedures to carry out security policies. In some cases, little or no direction is provided by this workbook for procedures below, but defined procedures are recommended for a mature IT process. Some of the most important specific operational areas to be addressed are included below. Chapter 6 includes sections for these and more:

**Roles and Responsibilities**: This section keeps track of the responsibilities that are assigned to each role, as work in the security workbook progresses. This is a good section to continually update, instead of working on this by itself. Start by defining the roles, even if no responsibilities are described.

**IT Equipment Inventory**: What computer/server/network devices does the organization own, and what specific hardware or software is loaded on each (particularly licensed software?)

**Standards or Procedures for Software Installation**: What standard set of software is installed for various IT users? How can users request specific software to be installed? What is the approval process for new software?

**Procedures for Back-up and Restore**: Data must be backed up on disk or tape, using a standard naming convention. Backed up data should be maintained off-site. Restore procedures describe how backup data can be reloaded in the event of a disk failure or sabotage.

**Procedures for Authentication & Access Control**: How are system/application permissions requested, approved, and tracked?

**Procedures for Incident Response**. This includes extended details for incident response.

**Procedures for Change Management**: How do people submit requests for changes?

Other Procedures: There may be other requirements (e.g., procedures, standards or guidelines) that are necessary to document.

## Permissions

This document is to be used as a workbook within a company or organization. However authorship rights and privileges remain with the author, Susan J Lincke, and her publisher Springer.

## Recognition of Contribution

The original development of this workbook was funded by the National Science Foundation (NSF) Course, Curriculum and Laboratory Improvement (CCLI) grant 0837574: Information Security: Audit, Case Study, and Service Learning. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and/or source(s) and do not necessarily reflect the views of the NSF.

My students and community partners have contributed greatly to this work by indicating areas requiring further clarification and explanation. Specific students have made significant contributions to one or more sections, including Tim Dorr and Gabriel John. I would like to thank the following people who have served as reviewers: Dr Weijun Zheng, Tim Knautz, Alice Pappas, and Natasha Ravnikar. Thank you to all contributors!

# Strategic Security Planning

The Strategic level is concerned with the business view, in order to determine what to protect and why. The strategic level gives a direction from executive management for security implementation. These strategic plans are defined or approved by upper management and disseminated to applicable employees, contractors, and volunteers.

## Identifying Security Issues and Legal Compliance

The first section of the *Information Security Planning* book discusses various information security and fraud threats. After reading these chapters, you should have ideas as to specific threats to your organization. Consider the general categories of experimentation, vandalism, hacktivism, cyber-crime, information warfare, and surveillance state. Before moving on, document them in the following tables.

### Identify Threat agents and Cyber Threats

Threat agents:

* Criminal (financial, spying)
* Nation-State (financial, spying, damage)
* Hacktivists (revenge)
* Experimenters
* Internal fraud

Cyber Threats: (Examples of: you may include others)

ransomware malware social engineering payment card exfiltration

hacking espionage database crack point-of-sale/ATM infiltration

DDOS coin mining physical penetration system/network failure/loss

damage IPR theft breach of regulation customer data breach

**Action**: List the cybersecurity threats that are likely to happen in your organization in the table below.

Table 2.1.1 General Cybersecurity Threats

|  |  |  |
| --- | --- | --- |
| **Threat Agent**  (e.g., Cyber-criminal, spy) | **Threat**  (e.g., PoS infiltration, stolen trade secrets) | **Impact**  (e.g., customer privacy breach, low-cost competitor) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Identify Fraud Threats

Also consider and list fraud threats to your organization, including internal or employee threats and external threats. General internal threats include: asset misappropriation, bribery and corruption, and financial statement fraud. External threats include social engineering, and receipt and financial instrument forgeries.

Internal Fraud Threats: (From ACFE 2020 Report to the Nations)

* **Corruption**: Conflict of interest, bribery, illegal gratuities, economic extortion
* **Asset Misappropriation**: Theft of cash on hand, theft of cash receipts (skimming, cash larceny), fraudulent disbursements (billing schemes, payroll schemes, expense reimbursement schemes, check and payment tampering, register disbursements), inventory/asset theft (misuse, larceny).
* **Financial Statement Fraud**: Net worth/income overstatement (timing differences, fictitious revenues, undisclosed liabilities and expenses, invalid asset valuations, improper disclosures), net worth/income understatements (timing inaccuracies, under-reported revenue, overstated liabilities and expenses, invalid asset valuations, improper disclosures).

**Action**: List the types of fraud threats that are likely to happen in your organization.

Table 2.1.2 Fraud Threats

|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Agent**  (e.g., vendor, employee, customer) | **Threat**  (e.g., theft, skimmer, social engineering) | **Impact** | **Control**  (e.g., segregation of duties, training, fraud hotline) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Identify Social Engineering Threats

What may be the goals of social engineers as a threat? Social engineering may include:

* **Phishing**: a first step to attain a foothold in the internal network by having employees click on links or open attachments; results in installed malware in the network.
* **Pretexting**: Social engineering used to create fraudulent accounts, obtain internal information, or exact favors within the organization, via phone, in-person or email accounts.
* **Business Email Compromise**: Take over an executive’s email account or impersonate an executive in a deep fake video conference, in order to demand payment or force a transaction.

**Action**: What types of social engineering threats are likely to happen in your organization?

Table 2.1.3 Social Engineering Threats

|  |  |
| --- | --- |
| Action or information to be gained | Example means of social engineering |
|  |  |
|  |  |
|  |  |
|  |  |

### Identify Applicable Regulation/Standards

Organizations must adhere to specific legislation, depending on industry. This section outlines regulations or standards related to information security, applicable to certain industries. Since this workbook is general in nature, it does not address specific issues related to particular regulations. This section addresses which parts of the textbook certain specific regulation requires.

**Regulation/Standards affecting many Organizations and Businesses**

**Payment Card Industry – Data Security Standard (PCI DSS):** These industry-oriented compliance standards are designed to protect customer-sensitive credit/debit card information. These standards protect full magnetic data or equivalent data on a chip, card validation code or value (CAV2/CID/CVC2/CVV2) and personal identification number (PIN) data.

**Breach Notification Laws**: Most U.S. states and territories require that if an organization divulges certain personal information, it is required to notify all affected persons. Commonly, this personal information includes Social Security numbers, driver’s license numbers or state IDs, financial account information, DNA, and biometric data.

**Specific Industries**

**Family Education Rights and Privacy Act (FERPA):** This federal law protects the privacy of student education records.

**Federal Information Security Management Act (FISMA):** This law ensures that information supporting the operations and assets of U.S. federal agencies are secured. This also applies to their contractors or contracting agencies.

**Gramm-Leach-Bliley (GLB):** Organizations handling financial accounts require security well beyond the reach of this workbook.

**Red Flag Rule**: Any organization that provides credit to customers, via credit card accounts, utility accounts, cell phone accounts, and retail financing plans, must adhere to this rule.

**Health Insurance Portability and Accountability Act (HIPAA/HITECH):** Medical and other organizations that handle patient records are affected, including doctors, dentists, psychologists, hospitals, and those ‘Business Associate’ organizations which work with these medical organizations. Any organization that retains patient records must adhere.

**Sarbanes-Oxley Act (SOX)**: Publicly-traded companies must adhere to this legislation. Non-profits must adhere to parts of this regulation.

**General Data Protection Regulation (GDPR):** If your organization does business in Europe, then this European regulation protects privacy and security in a comprehensive way.

**Action:** What regulations or standards should your organization be concerned with? Complete Table 2.1.4.

Table 2.1.4 Regulatory Concerns

|  |  |
| --- | --- |
| Regulation | Aspects of Organization:  Protected Information |
|  |  |
|  |  |
|  |  |
|  |  |

The table below outlines textbook chapters that should be addressed per regulation. In most cases, workbook section names are similar to textbook chapter names.

Bold or highlight the regulations that apply to your organization.

Table 2.1.5: Required (X) and Recommended (R) Textbook Sections

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Chapter  Notation: R=Required A=Advisable | State  Breach | HIPAA | SOX | GLB | Red  Flag | FISMA | FERPA | PCI DSS |
| 1. Security Awareness | A | R | R | R | R | R | A | A |
| 2. Fraud | A | A | R | R | R | R |  | A |
| 4. Risk |  | R | R | R | R | R |  | R |
| 5. Business Continuity |  | R | R | R |  | R |  | R |
| 6. Policy |  | R | R | R | R | R | R | R |
| 7. Information Security | R | R | R | R | R | R | R | R |
| 8. Network Security | R | R | R | R | A | R | R | R |
| 9. Physical Security | R | R | R | R | A | R | A | R |
| 10. Personnel Security |  | R | R | R | R | R |  | R |
| 11. Incident Response | R | R | R | R | R | R | A | R |
| 12. Metrics |  | A | R | A | A | R |  |  |
| 13. Audit |  | R | R | R | A | R |  | R |

**Question:** What chapters should your organization be concerned with? List them below.

## Managing Risk

This section evaluates, documents, and addresses risk that could cause substantial damage to the organization. Damage arises due to failures in confidentiality, integrity, and availability of resources. Managing risk is important for two reasons. First, it is the basis for the selection of cost-effective controls. Specifically, if you understand how much a security risk is expected to cost, you then know approximately how much you should pay to avoid or reduce that risk. Second, security legislation (e.g., HIPAA, SOX) expects organizations to expend ‘Due Care’ and ‘Due Diligence’ in addressing security, to assure the financial safety and privacy of clients and stockholders. Liability is minimized if reasonable precautions are taken.

**Vocabulary:**

The three major components of security to consider when working with risk include:

**Confidentiality:**  Data or resources are available only to authorized parties.

**Integrity:**  Data or resources are complete, accurate, and functional.

**Availability:**  Data or resources are available to be used when needed.

Security and privacy regulation demands:

**Due Diligence**: Perform a thorough and objective analysis of risk in a careful and responsible manner.

**Due Care**: Implement recommended and sufficient controls, as would be addressed by a reasonable person of similar competency under similar conditions.

The ultimate decision(s) of how risk should be managed is the prerogative of executive management. The steps of risk analysis include:

### Step 1: Determine Value of Assets (Crown Jewels):

The first step in risk analysis is to evaluate the value of the organization’s assets. Assets should be **prioritized,** with most important assets considered. Assets include:

* IT-Related: Information/data, hardware, software, services, documents, personnel
* Other: Buildings, inventory, cash, reputation, sales opportunities

**Direct Loss** considers replacement costs:

* How much would it cost to replace this asset? (Consider purchase, installation, recovery)

**Consequential Financial Loss** considers:

* How much of our income can we attribute to this asset?
* How much liability would we be subject to if the asset was compromised?
* What intangibles would we risk? Goodwill, reputation, future business?
* Does this asset have other value to the company?

**SLE = Single Loss Expectancy** = The cost to the organization if one threat occurs once

= Replacement Cost + Consequential Cost

Consequential Cost = liability/defense/goodwill + loss of business

**Action**: Complete Table 2.2.1 as per above directions. Below are some sample starter values you can modify, add to, or delete.

Table 2.2.1: Asset Value Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset Name** | **$ Value**  **Direct Loss: Replacement** | **$ Value**  **Consequential Financial Loss** | **Confidentiality, Integrity, and Availability Notes** |
| Building |  | 1D | Availability |
| Database |  | NL | Integrity, Availability |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Action**: You may include notes about the Consequential Financial Loss below:

Table 2.2.2: Consequential Financial Loss Calculations

|  |  |  |
| --- | --- | --- |
| Consequential Financial Loss | Total Loss | Calculations or Notes |
| Lost business for one day (1D) |  | Insert ‘1D x Duration’ in Consequential Financial Loss above |
| Privacy breach notification liability (NL) |  |  |
| Lawsuit (L) |  |  |
|  |  |  |

### Step 2: Estimate Potential Loss for Threats:

The second step is to determine the threats that could affect these assets. Threats that should be considered are listed below. **Circle the threats that are most important to your organization. Add threats specific to your industry as appropriate.**

Normal threats: Threats common to all organizations

Inherent threats: Threats particular to your specific industry

Known vulnerabilities: Previous audit reports indicate deficiencies.

Here are some categories and specific threats to consider:

Physical Threats

* Natural: Flood, fire, cyclones, hail/snow, plagues and earthquakes
* Unintentional: Fire, water, building damage/collapse, loss of utility services and equipment failure
* Intentional: Fire, water, theft and vandalism

Non-Physical Threats

* Ethical/Criminal: Fraud, ransomware, data breach, espionage, hacking, identity theft, malicious code, social engineering, vandalism, phishing and denial of service
* External Environmental: industry competition, contract failure, or changes in market, political, regulatory or technology environment
* Internal: management error, IT complexity, poor risk evaluation, organization immaturity, accidental data loss, mistakes, software defects and personnel incompetence.

Possible threat agents include people who perform intentional threats, such as: crackers, criminals, industry spies, insiders (e.g., fraudsters), and terrorists/hacktivists

**Vulnerabilities**are the ‘open doors’ that enable threats to occur. Categories of vulnerabilities include*:*

* Behavioral: Disgruntled employee, poor security design, improperly configured equipment;
* Misinterpretation: Employee error or incompetence, poor procedural documentation, poor compliance adherence, insufficient staff;
* Poor coding: Incomplete requirements, software defects, inadequate security design;
* Physical vulnerabilities: theft, negligence, extreme weather, no redundancy, violent attack.

Document your normal and inherent threats and known vulnerabilities in Figure 2.2.1 and Table 2.2.3.

### Step 3: Estimate Likelihood of Exploitation

Once we have listed the threats, we must determine the probability that they will occur. This is best evaluated using historical data, published figures, or if no figures are available, best guesses.

Is this likely to occur monthly, 1 year, 10 years, 20 years, 50 years?

Calculate **Annual Rate of Occurrence (ARO)** = How many times this is likely to occur in one year

The likelihood of each threat is documented in Figure 2.2.1 and Table 2.2.2. In Figure 2.2.1, be sure to include all threats, with estimated potential likelihood. It is possible to move the threats around that exist in the current diagram. It is also possible to expand the size of the diagram to consider all threats.

**Action**: You may move the different threats around in Figure 2.2.1 below to the appropriate quadrants. Make them applicable to your organization and geographic region.

Slow Down Business Temp. Shut Down Business Threaten Business

**2**

**3**

**1**

**4**

1 week

1 year

10 years

(.1)

5 years

(.2)

**Vulnerability**

**(Severity)**

20 years

(.05)

50 years

(.02)

**Threat**

**(Probability)**

Hacker/Criminal

Loss of Electricity

Snow Emergency

Malware

Pandemic

Tornado/Wind Storm

Failed Disk

Stolen Laptop

Stolen Backup Tape(s)

Flood

Social Engineering

Earthquake

Intruder

Fire

Figure 2.2.1: Vulnerability Assessment Quadrant Map

This table shows example values for some threats. The table can be expanded and modified as needed. Observe the time frame on the left side, and the impact levels on the top.

### Step 4: Compute Expected Loss

The next step is to prioritize the risks, according to their severity of impact. To accomplish this, it is best to calculate an annualized loss expectancy, using the Quantitative method in Table 2.2.3. If this is not possible, expected loss can be prioritized by using Figure 2.2.1 Qualitative Analysis of Risk. Relevant Quantitative equations include:

**Single Loss Expectancy (SLE)** = The cost of a single problematic event = Downtime + Recovery + Liability + Replacement

**Annual Rate of Occurrence (ARO) =** the probability or likelihood that that a SLE might occur during one year

**Risk Exposure** or **Annual Loss Expectancy (ALE)** = expected loss per year due to the threat = $\_Loss \* Probability(Vulnerability) = SLE x ARO

For example:

SLE(PC failure) = $1000 replacement + $1000 lost salary = $2000

Probability(PC failure) = once in 8 years = 1/8 or 12.5%

ALE(PC failure) = 0.125 x $2000 = $250 per year.

**Action**: Complete Table 2.2.3 below with estimated values for SLE and ARO. Example statistics are available in the text.

Table 2.2.3: Quantitative Risk Loss Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset** | **Threat** | **Single Loss Expectancy (SLE)** | **Annualized Rate of Occurrence (ARO)** | **Annual Loss Expectancy (ALE)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Step 5: Treat Risk

Once the risks are prioritized, we can treat the high priority risks, and accept the low priority risks. The steps include:

Survey & Select New Controls: Technical, managerial, or operational controls

Reduce, Transfer, Avoid or Accept Risk

**Risk Acceptance**: Handle attack when necessary

E.g., a comet hits

Ignore risk if risk exposure is negligible

**Risk Avoidance**: Stop doing risky behavior

E.g., do not use Social Security Numbers

**Risk Mitigation**: Implement control to minimize vulnerability

E.g., purchase & configure a firewall

**Risk Transference**: Pay someone to assume risk for you

E.g., buy malpractice insurance (doctor)

While financial impact can be transferred, legal responsibility cannot

**Risk Planning**: Implement a set of controls

**Risk Leverage** = (Risk exposure before reduction) – (risk exposure after reduction) / (cost of risk reduction)

The decision of how much risk to mitigate or accept is an executive management decision. Risk and controls should be addressed in Table 2.2.4: Analysis of Risk versus Controls.

**Question:** What approach to security controls is planned, and why?

**Action**: Complete Table 2.2.4, copying Risk and ALE Score from Table 2.2.3. Add controls for each risk.

Table 2.2.4: Analysis of Risk versus Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk** | **ALE Score** | **Control** | **Cost of Control** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Advanced: Deciding on Risk Tolerance:

Deciding what to treat, with many risks, is made easier with a risk tolerance scheme. Risks can be divided up into different priority levels or rails, e.g., high, medium and low with standard treatment as follows:

Table 2.2.5 Risk Tolerance Table

|  |  |
| --- | --- |
| **Risk Priority & Handling** | **Qualifications for Priority** |
| High Risk: Always treated |  |
| Medium Risk: Negotiable  Decided individually by management |  |
| Low Risk: Always accepted |  |

Decisions that need to be made per treatment class include:

* Financial impact: A range of ALE costs for a risk
* Reputational impact: Impact on public perception if risk were to occur
* Legal impact: Adhering (or not) to a regulation or standard

Another consideration is how risks may be handled; may they be transferred (via insurance) or must they be mitigated or avoided?

High or medium priority risks may not be managed at a given time, due to insufficient technology, finances or personnel. In that case, **Risk Exceptions** are signed off on and reviewed regularly (quarterly or annually) for specific unhandled risks.

Table 2.2.6: Risk Exceptions

|  |  |  |
| --- | --- | --- |
| **Risk Priority & Description** | **Reason for Exception** | **Management Sign-off** |
|  |  |  |
|  |  |  |

A good system for handling risks is a Integrated Risk Management database, also known as a Governance Risk & Compliance (GRC) database. These can track all information about risks, including its priority and exception handling.

## Addressing Business Impact Analysis & Business Continuity

Are there parts of the business that if the computer system failed would cause service disruption and severe distress? Business Continuity defines how an organization will cope if a computer server or site or network goes out-of-service. Some services absolutely require real-time computer services, while other services do not.

In this section, we want to consider what could go wrong (as best as possible), and how to reduce impact and recover from any such occurrence. First, we must determine which business functions are high priority to the organization, and are susceptible to system failure. We then must be creative in planning potential workarounds, and then document the steps required to recover the IT systems. (Documented procedures are best since one never knows who might be required to perform them!) Finally, it is a good idea to test these plans in a controlled way. Three important documents include:

**Business Impact Analysis**: An analysis of which business functions and finances would be most affected by a problematic event or disaster.

**Business Continuity Plan**: A business plan for how the organization should resume service, following a disaster.

**Disaster Recovery Plan**: A technical plan for how IT should resume service following a problematic event or disaster.

### Business Impact Analysis

#### Step 1: Define Threats Resulting in Business Disruption

Key questions that are of importance are (some of which may be borrowed from the previous section on risk):

* Which business processes are of strategic importance?
* What disasters could occur?
* What impact would they have on the organization financially? Legally? On human life? On reputation?

Answers should be obtained via questionnaire, interviews, or meeting with key users of IT. While answering these questions, consider that threat categories and samples are listed below, but their impact on business must be determined:

* System failures: server, network, or disk failure;
* External/weather: storms, tornado, earthquake, fire, electric failure;
* Hacker attack: malware, Distributed Denial of Service, penetration;
* Employee negligence or fraud: incompetence, error, revenge.

Other threats may have been identified in the Risk section.

For each disaster or problematic event, the impact can be categorized using the following **Impact Classifications**:

**Crisis**: Has a major material or financial impact on the business

**Major**: Impacts one or more departments and may impact outside clients

**Minor**: A non-negligible event with no material or financial impact on the business

**Negligible**: No significant cost or damage

**Action**: Complete Table 2.3.1, which considers the threats that may affect your business processes. You may add or subtract problematic events applicable to your organization. Types of business processes may include: Sales, Engineering, Shipping, Accounting, etc. but should be appropriate for your organization.

Table 2.3.1: Incidents and Impacts

|  |  |  |
| --- | --- | --- |
| **Problematic Event or Incident** | **Affected Business Process(es)** | **Impact Classification**  Effect on finances, legal liability, human life, reputation |
| Fire |  |  |
| Hacking intrusion (re: availability) |  |  |
| Network Unavailable |  |  |
| Server Failure  (Disk/server) |  |  |
| Power Failure |  |  |
| Loss of Cloud |  |  |
| Fraud, social engineering (re: availability) |  |  |
| Server room flood or fire |  |  |

#### Step 2: Define Recovery Objectives

The next major question is: what is the required recovery time period?

Consider Figure 2.3.1. Following an IT interruption, how long can you afford to operate without IT system services? The Recovery Time Objective defines when you need an alternate system operational in order to constrain business loss.

If a disk failure occurs, you will likely lose all recent data updates made since the last backup. This lost data is called ‘**orphan data**’. The Recovery Point Objective defines how far back you are willing to lose data, if an unfortunate event occurs to your disk.

Figure 2.3.1 RPO and RTO

One

Week

One

Day

One

Hour

One

Hour

One One

Day Week

Recovery Point Objective

Recovery Time Objective

Measures lost or ‘orphan’ data from *before* the interruption

Measures lost processing time *after* the interruption

Interruption

Required vocabulary for this section includes:

**Recovery Point Objective (RPO)**: Data or transactions may be lost if a disk failure occurred. For example, consider that you do homework all day and when you get the project done, your disk fails or your laptop is stolen or your lose your memory stick; in this case you would have lost all of your assignment. Similarly, banks and stores can lose transactions. For what duration of time can the organization afford to lose data for each service? This will define in part how often backups are performed.

**Recovery Time Objective (RTO)**: Some business functions must resume immediately at a backup location and backup computer, while other functions can be manually performed for extended periods after such a failure.

**Service Delivery Objective (SDO)**: When the primary system is not functional, and the secondary system is running, what services and service levels should be supported on the secondary (or alternate) system?

**Action**: In Table 2.3.2 below, list the prioritized business processes (with impact classifications of Crisis or Major) with your desired RPO and RTO. What resources do you depend on for full functionality? Are there special times of the month, year, or special events?

Table 2.3.2 Business Impact Analysis Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Business Process** | **Recovery Point Objective**  (Hours) | **Recovery Time Objective**  (Hours) | **Critical Resources**  (Computer, people, peripherals) | **Special Notes**  (Unusual treatment at specific times, unusual risk conditions) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

The RTO determines the **Criticality Classification** of the process and its information:

**Critical**: Cannot be performed manually. Tolerance to interruption is very low

**Vital**: Can be performed manually for very short time

**Sensitive**: Can be performed manually for a period of time, but may cost more in staff

**Non-sensitive**: Can be performed manually for an extended period of time with little additional cost and minimal recovery effort

### Step 3: Plan for Recovery (Business Continuity)

Now that we understand our critical business functions, it is time to determine how best to minimize potential problems and to reduce recovery times. The approach to business continuity needs to be considered. Three approaches to business continuity include:

* High availability solutions: Relies upon active redundancy to reduce the probability of outage: if a failure occurs, your alternate solution takes over. This solution is best for critical and vital services.
* Recovery sites: Relies upon an alternate backup site: if a first site fails, a planned second site is configured and brought up.
* Cloud Computing:A cloud provider be contracted to run your services at high availability, or can serve as a backup site for you.
* Backup: Backups are critical regardless of the type of Business Continuity solution used. Employee error, disk failures, and/or malware may corrupt your disks, requiring recovery from a backup media.

Here are specific solutions to consider:

|  |  |
| --- | --- |
| **High Availability Solutions** | **Recovery Sites** |
| RAID: Redundant Array of Independent Disks: Redundancy at single site | Duplicate Information Processing Facility |
| Storage Array  Data sharing and migration between different sites. | Reciprocal Agreement (with another organization) |
| Fault tolerant servers  E.g., clusters: distributed processing (active-active), standby configuration (active-passive) | Commercial backup:   * Hot site: within hours * Warm site: within days * Cold site: within weeks |
| Network redundancy  E.g., diverse routing, alternate routing | Mobile facility |
| Cloud services (depending on agreement) | |

**Question**: What are feasible options for you? Describe feasible ideas here:

**Step 3B: Attaining Recovery Point Objective (RPO)**

The RPO defines the backup period for data.

**Action**: Complete the following table:

Table 2.3.3. RPO Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Process** | **RPO**  (Hours) | **Criticality Classification** | **Special Treatment**  (Backup period, RAID, File Retention Strategies) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Backup:**  Data is saved periodically to another memory (e.g., CD/DVD, tape, second disk drive, or another system computer). Two types of backups may occur:

* **Complete backup:** The full disk or set of directories are copied
* **Partial backup**: Only the updates since the last backup are copied

Considerations for backup include:

Backup tapes or disks should be labeled and retained off-site in a temperature-controlled, secure location.

If partial backups are used, complete backups should periodically be taken (e.g., weekly).

If backup data contains Personally Identifiable Information, the backup data should be encrypted.

Special questions that must be answered in a low level procedure (in Chapter 5) include:

* Who is responsible for performing backups?
* Where are backups retained off-site?
* How many backups are retained, and how are they rotated?
* What is the naming convention for backup media?
* How is the backup and recovery process tested?

Procedures describing the backup and recovery processes shall be defined.

Backup and recovery procedures must be defined in Section 5 of this document.

**Step 3C: Business Continuity: Attaining Recovery Time Objective (RTO)**

If the organization has Critical or Vital data classifications, this section must be considered. Table 2.3.4 defines the Critical and Vital services, which will require immediate action if disaster or major problems occur. At this point you should be able to complete the first 3 columns.

**Action**: Complete Table 2.3.4. Start with the first 3 columns, then add an outline of the procedure as it becomes apparent.

Table 2.3.4: Business Continuity Overview

|  |  |  |  |
| --- | --- | --- | --- |
| **Criticality Classification**  (Critical or Vital) | **Business Process** | **Incident or Problematic Event(s)** | **Procedure for Handling**  (Section 5) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

The next consideration relates to how you can use this site to conduct business (Business Continuity) and perform computer operations (Disaster Recovery): Special vocabulary includes:

**Alternate Process Mode**: Business service offered by a backup IT system

**Disaster Recovery Plan**: How to transition to Alternate Process Mode (IT considerations)

In Section 5 you should specify these Business Continuity and Disaster Recovery Plans. Also list these plans in the last column of Table 2.3.4, above. Considerations for a detailed implementation in Section 5 include:

* Determine alternate processing modes for critical and vital services
* Develop the Disaster Recovery Plan for IS systems recovery (in Section 5)
* Develop BCP for business operations recovery and continuation (in Section 5)
* Test the plans
* Maintain plans

A competent system administrator can help to write detailed procedures for backup/recovery and disaster recovery, and configure backup systems (e.g., RAID).

## Governing with a Policy Manual

A professional policy manual can be found at the National Institute for Science and Technology website, for: NIST Cybersecurity Framework 1.1 Excel spreadsheet (in new reference directory). This set of policies is only good as a starter point for small businesses.

Policies provide management direction for the organization. Policies for the IT department included below are based at a high level on IT maturity standard COBIT version 4 level 3, but applied to a small business. Policies applying to business functional areas should also be addressed. After policies are defined, specific procedures, guidelines, or standards shall be developed to ensure conformity.

This section includes policies and shorter standards. More detailed standards, guidelines and procedures should be documented in Chapter 5. Definitions:

1. **Policy**: General high-level rule offers direction, provided by executive management
2. **Standard**: Detailed or applied rule
3. **Guideline**: Recommendation
4. **Procedure**: Step by step guide (how-to)

**Action**: **You may edit this policy according to your own needs and/or capabilities, and expand as your organization matures.**

Recommendation: There should rarely be more than 24 policies. Often small organizations have understood rules, which should be written down. These can often be used as a starting point for policy development.

### IT Strategic Planning

IT Strategic Planning ensures that IT meets organizational needs and goals. The strategic planning process occurs annually between enterprise and IT management, and includes discussion of business expectations and IT resource needs and risks. IT prepares a report on technology and security, which is also reviewed by the board of directors. An IT Steering Committee addresses tactical planning, and consists of business management, IT, and information security management.

#### Standard: Strategic Planning

Strategic planning discussion areas shall include:

1. Review of planned versus actual budget for previous year, and budget expectation for future year.
2. Review of planned versus actual achievements for previous year and goals for future year.
3. Technological advances, migration, and contingency of technology infrastructure.
4. Financial, technical, security and human resource requirements of IT

#### Standard: The IT Steering Committee

The IT Steering Committee addresses tactical planning periodically (at least twice a year for very small organizations). Discussions address:

1. Status reports on risk, budget, measures
2. Changes in IT management, including changes to staff roles and responsibilities, data classification, and changes impacting risk
3. Technology infrastructure plans or new, major proposals
4. Project progress

### Security Management

Policy definition is used to achieve legal compliance and adherence to PCI-DSS and COBIT level 3, the Defined Level, applied to small business. Policies ensure that all legal obligations are addressed and fulfilled. Each security policy is further defined by policies, standards, and/or guidelines. These security policy definitions are maintained in an online directory, which is accessible to all on a need-to-know basis. Paper copies of the applicable policies are provided at hiring, and the new hire signs a statement that he/she will adhere to policy definitions.

#### Standard: Security Documentation

Security documentation is retained online at (for example) F:/security-documents. F:/security-documents holds the Policies file and additional directories, which contain procedures for specific organizational functions.

### Information Asset Protection

Information assets are protected for confidentiality, integrity, and availability. Information assets are identified and classified by criticality and sensitivity: Information assets pertaining to the operation of the business are cataloged, including listing the owner, value, and classification of data criticality and sensitivity.

#### Standard: Data Classification

Data classification describes how data is categorized into classifications, and the handling of each class of data. Classification identifies categories requiring encryption in storage, transmission, and archive.

### Risk Management

Risk Management is used to protect the organization via cost-effective controls. Risk Assessment is reviewed at least annually within the IT Steering Committee. Controls are evaluated for efficiency and cost-effectiveness, and residual risk is accepted by executive management.

### Access Control

Least privilege ensures that information access is provided only on an as-needed basis. All computer access requires individual authentication, and access to software, hardware, and data is controlled. Data owners determine who has access to data views (or which roles can view/access which data.)

#### Standard: Areas for Access Control

1. Authentication requires a unique login ID per person and complex passwords of 14 characters in length
2. A filter (e.g., firewall or border router) protects access to the internal network from the internet
3. Guideline: Passwords must be changed every 3 months and a password history should accommodate a memory of 5 passwords.

### System Security

Due diligence requires that computer security is professionally accomplished, according to risk management. System security requires technological and management controls, including logging, security patching, antivirus software, security testing, as well as security functions mentioned elsewhere: firewalls, authentication, incident response, security testing, and encryption. Security incidents are categorized and approaches to incident handling are documented. Escalation of incidents ensures management awareness of security problems.

#### Standard: Security Testing

A risk-based plan for security testing is prepared, and testing occurs minimally once per year.

### Human Resources

Employee management prevents fraud and undesirable action. Procedures define the hiring, employee review, and termination process. Employee roles are documented, and critical dependencies on key personnel are minimized via segregation of duties or job rotation. Training for security, legal, and contractual obligations are defined, performed, and tracked. Employees shall be made aware that consequences of disobeying policies may range from censure to job termination, legal actions, and/or reporting of incidents to police.

#### Standard: Training

Position definitions list education and training qualifications, and describe any training that is required upon hiring. Security awareness training is provided to new hires and is re-reviewed annually. Security training is required annually by IT security staff. Training for legal and contractual obligations is defined.

### Business Continuity

Business continuity ensures that critical business can continue even after disaster strikes. The Business Continuity Plan (BCP) is based on a Business Impact Analysis, which analyzes which business functions are critical and rely on computer and other resources. Review of the BCP and some form of testing occurs annually. A Disaster Recovery Plan describes IT procedures for recovery. Backup/recovery procedures are defined and tested, and critical data is backed up and retained off-site. Responsibility is allocated for the development, management, and execution of these functions, and this role is commonly known to employees. All plans are retained on-line and via paper-format, both on-site, and off-site.

#### Standard: Backup/Recovery

Procedures for backup/restoration include identification of data to be backed up, description of retention period, and method of disposal of backup data. Responsibility is allocated.

### Physical Controls

Security shall ensure that physical access is restricted to computing resources and physical documents requiring protection. Physical security includes consideration of human attack, and fire, water, and electrical or network failures.

#### Standard: Physical Map

A map shall be designed showing computer facilities, physical controls, and access restrictions, including locked doors, fire suppressants, air conditioning, and surge protectors or UPS.

### Change Management

Changes to computer systems (hardware and software) are tracked to ensure business can effectively use computer services, and to enable and ensure that IT and IS functions provide those capabilities. A process for requesting changes is defined and all changes are logged. Responsibility is allocated. Change is defined to include IT service affecting machines or software. Change requests are categorized, prioritized, and authorized. Requested changes are documented, and rejected or approved and implemented, including a response to the originator.

### Internal Control

Internal control ensures adherence to law and regulation, contractual obligations, and organizational policies. Internal control is planned according to risk profiles, and assessment occurs at least annually. Areas to be addressed include security controls, legal obligations, and third party contractual obligations. Staff members are audited (i.e., interviewed) to ensure compliance with legal and contractual requirements.

#### Standard: Internal Audit

An outline is defined for internal audits in Section 4.

### Software/Hardware/Service Acquisition & Management

Software and hardware adaptation is controlled to ensure quality, security, and effectiveness. The IT procurement process adheres to the standard business procurement process. A feasibility study evaluates alternative implementations for all products exceeding $1000. Major software or infrastructure purchases are planned and managed. Products directly related to business functions are always tested before implementation. Users provide feedback via questionnaire responses. Documentation is maintained in a standard location, available to parties requiring access. Software and hardware assets are tracked, including maintenance changes. *Additional policy statements are required for software development.*

#### Standard: Procurement requirements:

1. Requirements are documented in advance of product selection.
2. Vendors are selected via a review process involving multiple candidates.
3. Requirements for contracts are followed.

#### Standard: Software Testing

Acquired or developed software is tested.

1. Test plans are written, executed, and results documented.
2. Software is tested and approved before software is moved into production.

### Third Party Services

Contracts and relationships with third parties are controlled and managed for contract adherence, security, and risk.

#### Standard: Third Party

Requirements include:

1. Specification of capacity requirements, risk and security
2. Review of multiple providers during selection process
3. Disclosure of unusual relationships during the product selection and oversight process
4. Allocation of responsibility for oversight of third party relationship
5. Maintenance of contracts, SLA, and documents describing responsibilities, goals, deliverables
6. Retention of written communications between the two organizations
7. Documentation of problems and exceptional performance
8. Performance monitoring is reported quarterly

### IT-IS Management

Effective management is required for the IT and information security functions. The IT/IS manager(s) have project management training, and follow the project management methodology used by the rest of the organization. IT/IS receives business input in plan development. IT operations include a description of tasks and responsibility allocation. Responsibilities include log monitoring and equipment maintenance.

### Process Improvement

Measures (or strategic IT statistics) enable process improvement in the organization. Measures are defined by business and IT management. Measures are tracked and reported upon, and historical progressions are analyzed.

### Legal and Contractual Obligations

The organization adheres to regulation and contractual obligation. Policy is consistent with regulation and long-term contractual obligations. Procedures exist and personnel are trained for adherence.

#### Standard: PCI DSS Adherence

PCI DSS adherence is required to accept credit card charges. The full scope of this policy is not addressed by this Workbook. Instead, see *Payment Card Industry Data Security Standard: Requirements and Testing Procedures* at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Preparing a Code of Ethics

This code of ethics[[6]](#footnote-2) provides general guidelines, and is not intended to cover every potential scenario. Examples are provided only as necessary for the employee to understand general concepts.

**Action**: You may add and edit to provide specific guidelines for your organization below.

#### General Employee Conduct While at Work

This organization expects employees to be honest and ethical at the work place, and to guide their actions while employed by this organization.

#### Unethical Behavior

The organization has a zero-tolerance level for unethical and illegal behavior. Violations will result in censure, termination, and/or legal action, depending on the violation. Strictly prohibited behavior includes (but is not limited to) taking kickbacks or bribes, giving confidential information to parties outside the company, falsifying employment documents, or other unethical actions as specified below.

#### Conflict of Interest

Are there any employee actions or relationships that may undermine work at this organization?

#### Confidentiality

What information should not be shared between departments or to the outside?

#### Relationship with Customers and Suppliers

What kinds of relationships are allowed between employees, vendors, and customers?

#### Gifts

What gifts may be received from outside persons? Up to what $ amount?

#### Entertainment

What types of entertainment activities are permitted or not, and how often may they occur?

#### Using the Organization’s Assets for Personal Activities

Some limited use of company computers and copiers for personal use may be allowed. Any office supplies, Internet use, copier and vehicle use that are not allowed for personal reasons should be described here.

#### Reporting Fraud or Unethical Behavior

This organization has an open-door policy particularly related to unethical behavior or fraud. Report all unethical behavior or fraud to <contact name> at <email> or <phone>. This organization has a policy of keeping such reports confidential. Alternatively, anonymous tips may be mailed to <contact name> at <address>.

# Tactical Security Planning

Tactical security is planned after the strategic level has defined the general security direction and priority. At this planning level, medium level security decisions are made, including for information security, network security, physical security, and metrics. The most detailed level is the Operational level, which may occur simultaneously with or after this level.

For this section it may not be possible initially to define all sections perfectly and completely. It is usually better to address the most critical areas of the business well, than to spend time doing a complete job on all aspects of the business.

## Designing Information Security

This section describes the protection of organizational data that is of strategic or critical importance. The goals are to ensure segregation of duties to prevent fraud, and protect data that must remain confidential for legal, liability, business competition, trade secret, goodwill and/or reputational reasons. General security rules include:

**Segregation of Duties:**  To reduce the probability of fraud, no single person should be able to subvert the system. Roles are divided into **Origination, Authorization, Distribution, and Verification**. (E.g. At a theater an ‘Origination’ person sells you the ticket, a ‘Distribution’ person collects tickets.)

**Need-to-Know**: People should be able to access only the information that they absolutely require in order to complete their job functions.

**Least Privilege**: Persons should have the ability to do tasks (read, create, modify, delete, and/or execute) sufficiently to perform their primary job and no more. (E.g., if someone needs to read a record but not to write to it, then only read permissions should be granted.)

**Data is a Liability**: Personal private information is a liability. Such information should be kept for a minimal time, or not at all, if possible.

**State Breach Law**: Protects Personally Identifiable Information (PII), which usually includes: Social Security number, driver’s license number or state ID number, financial account number or code enabling access to individual’s financial account, DNA profile, and biometric data. **Breach notification laws** require notification of breach to affected individuals. However, this may not be required when devices with PII (e.g., laptop, backup tapes) are encrypted.

Finally, to do this section completely may take considerable effort, often more time than is available. **Using time effectively means prioritizing the most important data first**: that data which is highly critical and/or sensitive. Some data may never be fully analyzed.

Data classifications are defined as standards for how each category of data is to be handled. Data can be classified by both their criticality (interruption tolerance) and sensitivity (privacy). These standards include who should have access to confidential or critical data, and how authorization is to be handled to ensure access is limited.

### Step 1: Classify Data for CIA

Data classification related to criticality is associated with business impact assessment, and which data is most sensitive to interruption.

**Critical**: Cannot be performed manually. Tolerance to interruption is very low

**Vital**: Can be performed manually for very short time: e.g., 4 hours

**Sensitive**: Can be performed manually for a period of time (e.g., 2 days), but may cost more in staff

**Non-Sensitive**: Can be performed manually for an extended period of time with little additional cost and minimal recovery effort

#### Classifying Sensitivity

Data classification related to sensitivity is associated with privacy, liability, and proprietary secrets. Most companies use 3-4 classifications (minimizing categories).

Which classes apply to you?

Which classes does your information fall into?

**Action**: Update Table 3.1.1 to apply appropriately to your organization.

Table 3.1.1: Sensitivity Classification

|  |  |  |
| --- | --- | --- |
| **Sensitivity**  **Classification** | **Description** | **Information Covered** |
| Proprietary | Protects competitive edge. Material is of critical strategic importance to the company and its dissemination could result in serious financial impact. | Trade secrets such as  Commercial program code or  List of sales customers  Marketing plans |
| Confidential | Information protected by law. Shall be made available or visible on a need-to-know basis only. Dissemination could result in financial liability or reputation loss. | Personally Identifiable Information (PII or private info)  Payment card information  Personnel records |
| Privileged | Should be accessible to management or for use with particular parties within the organization. Could cause internal strife or divulge trade secrets if released. | Project plans, Budgets  Engineering designs, test plans  Supply orders |
| Public | Disclosure is not welcome, but would not adversely impact the organization  OR  Information is public record | Meeting information  Sales brochures  Release dates (before finalized) |

#### Asset Inventory

Now we inventory the assets or data repositories, allocating criticality and sensitivity classes for each and defining who allocates permissions, has access to assets, and asset classifications.

**Data Owner**: Determines who can have access to data and may grant permissions directly OR gives written permission for access directly to security/system administrator.

**Data Custodian**: The position or person responsible for protection of the physical data (e.g., backup procedures, technical protection).

**Data User or Granted Permissions**: Which roles may access this file? Mandatory Access Control determines in general who can access the file or database. A later section, Role-Based Access Control, will determine which roles can have specific access to selected parts of the data (e.g., specific database forms). The next sections explain this more fully.

**Action**: For coursework, please define two assets for a highly critical, highly sensitive application, using copies of Table 3.1.2.

Table 3.1.2: Asset Inventory

|  |  |
| --- | --- |
| **Asset Name** |  |
| Functional Value to Organization |  |
| Location |  |
| Criticality and Sensitivity Classifications |  |
| IS System/Server Name |  |
| Data Owner |  |
| Designated Custodian |  |
| Granted Permissions |  |

|  |  |
| --- | --- |
| **Asset Name** |  |
| Functional Value to Organization |  |
| Location |  |
| Criticality and Sensitivity Classifications |  |
| IS System/Server Name |  |
| Data Owner |  |
| Designated Custodian |  |
| Granted Permissions |  |

### Step 2: Allocate Controls

Special controls that can be added at the Sensitivity Class specification level (Handling of Sensitive Data Table) or at the individual file level (Inventory) include the following controls:

|  |  |
| --- | --- |
| **Control** | **Systems** |
| Authentication | Complex passwords, multifactor authentication, biometric systems. |
| Access Controls | Mandatory, role based, attribute based, physical and/or discretionary access control |
| Accountability | Logs, transaction audit trails, attack signature detection, trend variance detection |
| Audit | Checking policies, processes, staff awareness and security training via official audits; management reports monitor accountability |

#### Treatment of Sensitive Data

Shown is example treatment, which should be personalized.

**Action**: Personalize Table 3.1.3 for your organization.

Table 3.1.3: Handling of Sensitive Data

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Proprietary** | **Confidential** | **Privileged** |
| Access | Need to know  Multifactor authentication | Need to know  Multifactor authentication | Need to know  Password-protected |
| Paper Storage | Locked cabinet,  Locked room if unattended | Locked cabinet  Locked room if unattended | Locked cabinet or locked room if unattended |
| Disk Storage | Encrypted  Camera monitor for server rooms | Encrypted | Password-Protected |
| Labeling and Handling | Label ‘Proprietary’,  Clean desk,  low voice,  shut door policy | Label ‘Confidential’  Clean desk,  low voice,  shut door policy | Clean desk,  low voice,  shut door policy |
| Transmission/ Migration | Encrypted with integrity checks | Encrypted with integrity | No requirements |
| Email Handling | No email transmission | No requirements | No requirements |
| Data Warehousing | De-identification occurs through summary reports based on course summaries or major summaries | Not applicable | N.A. |
| Archive & Retention | Encrypted with integrity checks | Encrypted with integrity checks | Encrypted |
| Disposal & Destruction | Degauss & damage disks  Cross-shred paper/ incinerate | Write patterns to disk, damage disks  Cross-shred paper | Reformat disks |
| Bring your own Data | Not allowed | Local storage copies are not allowed | Files and documents may be written and read but not copied to local storage media. |
| Cloud Storage | Ensure SLA is regulation compliant while allowing regular audits. Meets above requirements. |  | Use least privilege access. Monitor access logs for unauthorized access |
| Employee Termination | Purge access rights  Ensure no data exfiltration before employee release | Purge access rights | Purge access rights |

Disposal notes: Reformatting disks is not a reliable form of wiping data. Better forms include degaussing (demagnetizing disks), secure wipes and shredding or fully damaging disks.

#### Considering Regulations Associated with Data Assets

This area is industry-specific, and lists specific regulations associated with information protection, usually affecting security, availability, and retention.

### Step 3: Allocate Roles and Permissions

#### Defining Roles

Role-based access control implements the security concept of Least Privilege. With role-based access control, we first define various roles and their business functions. Examples of roles include: personnel, factory worker, engineer, nurse, teacher, manager or administrator. We can use these roles to define permission to access data, or access control. It may be good to work simultaneously on Section 3.8 Organizing Personnel Security.

**Action**: Complete Table 3.1.4 for your organization, listing information for main roles.

Table 3.1.4: Table of Roles

|  |  |  |
| --- | --- | --- |
| **Role Name** | **Role Description** | **Current Staff**  (Example or complete staff) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

#### Using Role-Based Access Control

Best practices in security dictates Need-to-Know and Least-Privilege: roles shall have minimal access sufficient to do their job.

**Action**: In Table 3.1.5, consider what minimum functions and access would be for each role. Who can read and/or write to which forms? Are there special fields on the forms which roles shall not access?

Table 3.1.5: Role-Based Access Control

|  |  |
| --- | --- |
| **Role Name** | **Information Access** (e.g., Record or Form Name)  **and Permissions** (e.g., Read (R) Write (W) Execute (X)  Can include: Create (C) and Delete (D)) |
|  |  |
|  |  |
|  |  |
|  |  |

**Attribute-Based Access Control**: Access control for roles may not only be defined per form and report, but also be defined per attribute or field on forms. Thus, some roles will have different permissions to read/write for specific fields or forms.

Professional system administration personnel should assist in configuring permissions and encryption, for destroying or removing memory when necessary, and for ensuring system security, as defined in Section 5.

## Planning for Network Security

Network security considers where requests enter the internal network, where they are processed, and what controls exist and where. Here are security considerations for network security:

**Defense in Depth**: Just as a castle is defended with multiple layers (moat, high wall, stone exterior, guards, single entrance drawbridge, etc.), an IT system also has multiple layers: firewall, antivirus, authentication, strong encryption, access control, logged problems, etc. Your servers and computers should be configured to support the required applications and no more (providing less features to attack!)

**Least Privilege**: The network context minimizes network access to absolute necessary services. For example, firewalls should limit outsider access to specifically-permitted applications. This is also known as **Default Deny**.

**Compartmentalization:** If hackers break into one part of a network, they are likely to be able to escalate their attack to other computers in that network’s region. By separating network regions or ‘zones’ using firewalls, one can ensure that if a break-in does occur, other services are not affected. The same is true for servers: once one service is broken into, it is easier to break into other services on the same physical machine. Thus, it is helpful to allocate different services on different physical servers.

**Fail-closed**: If equipment fails, service stops. For example, a firewall failure may allow in all packets or no packets. With fail-closed, no packets are allowed to enter.

### Step 1: Determine Services and Devices which may Enter and Leave the Network

We want to permit only legal transactions in our network. The purpose of the firewall is to enforce only these permissions. Thus, firewalls achieve Least Privilege and minimize hacker access. First, we consider which internal services can be accessed from the outside (i.e., Internet), and which services employees can access in the internal and outside networks. Secondly, we define where in the Internet the services can be accessed from. We want our firewalls to restrict access to specific services and preferably known IP addresses (as opposed to the whole world).

**Step 1**: Draw a rough sketch of the organization’s network. Include internal network computers or rooms, as well as important external (Internet) entities. Label lines/arrows with service names and have arrowheads point from the source/originator to the destination. Draw communication arrows/lines in red (or another special notation) for sensitive services that must be encrypted. For example, a ‘web purchase’ service is a label over a red arrow, which points to the ‘web sales server’ from ‘public’ and ‘internal staff computers’.

**Step 2**: Complete Table 3.2.1 with what you have learned in Step 1.

*Table 3.2.1: Identifying Sources and Destinations for Services*

|  |  |  |
| --- | --- | --- |
| **Service**  (e.g., web, sales database) | **Source**  (e.g., home, world, local computer) | **Destination**  (local server, home, world, etc.) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Note: At first pass, consider only the main services. Later on, you can also add other transactions, such as software updates (e.g., for the operating system and other applications.)

Also answer the following questions, in references to devices in the network:

* What devices are permitted in the network?
* Rogue wireless access points?
* New terminals, servers?
* Bring Your Own Device?
* Particular areas where external devices will be permitted?
* What is required configuration for permitted devices: allowed software, website accesses?

Notes:

### Step 2: Determine Sensitivity of Services

To achieve Compartmentalization, the decision of whether services (or applications) should be separated or confined must consider the similarity of: 1) the data’s sensitivity classifications, 2) the roles which may access the service, and 3) the probability of any specific service being attacked. For example, e-mail is a service highly likely to be attacked, and should not be housed with sensitive services.

* **Sensitivity Classes: Proprietary, Confidential, Privileged, Public**
* **Criticality Classes: Critical, Vital, Sensitive, Non-sensitive**

In Table 3.2.2, consider which services (or applications) require which sensitivity ratings and role access. Services with different roles and sensitivity classes should be separated onto different physical or virtual servers. With this in mind, consider which computers or servers the services should be hosted on, and provide a name for its server.

Sensitive services are first quarantined using separate physical or virtual computer systems and disks. Thus, if an attacker breaks in, they only access a limited set of data.

**Virtual Server**: Putting one service per (physical) server is very secure – but also expensive since it requires lots of physical computer servers. A safer way to consolidate services on one physical server is to compartmentalize services onto different *virtual* servers, which are then combined onto one *physical* server. Each *virtual* (or logical) server has its own operating system and access to a limited section of disk. Virtual systems can be achieved using software like VMware.

**Action**: Complete all columns of Table 3.2.2 for your organization. You may make up Server Names.

Table 3.2.2: Identifying Service Classifications and Roles

|  |  |  |  |
| --- | --- | --- | --- |
| **Service Name**  (E.g., Web, Email) | **Sensitivity Class**  (E.g., Confidential) | **Roles with Access**  (E.g., Sales, Eng.) | **Server Name**  (\*=Virtual) |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Step 3: Allocate Network Zones

Compartmentalization can occur using network zones, in addition to separate servers.

**Network Zones**: Networks are often divided into regions. Each region will correspond to a related Sensitivity Class, access roles, and accessibility. Accessibility refers to the probability of being broken into: networks with wireless access, the Internet, and public services are higher risk. A **Demilitarized Zone (DMZ)** is a region in a network that is accessible to the public, e.g., for web and e-mail services. One or more private zones restrict public access. Larger organizations have (at least) one zone per functional area: e.g., manufacturing, engineering, personnel. In Table 3.2.3, you may add or delete zones as necessary.

**Firewall** or **Border Router**: Firewalls serve as guards between zones, restricting access to only what is allowed. They limit or filter application transactions that enter and leave individual network zones. Minimally they filter packets by source or destination (IP) address, and service type (or port number).

**Action**: Update Table 3.2.3 for your organization, by modifying zone descriptions and adding or deleting zones as appropriate.

Table 3.2.3: Creating Zones

|  |  |  |
| --- | --- | --- |
| **Zone** | **Services** | **Zone Description**  (You may delete or add rows as necessary) |
| Internet  (External) |  | This zone is external to the organization. |
| De-Militarized Zone | Web,  Email,  DNS | This zone houses services the public are allowed to access in our network. |
| Wireless Network | Wireless local employees | This zone connects wireless/laptop employees (and possibly crackers) to our internal network. |
| Privileged Server Zone | Databases | This zone hosts our privileged sensitive server information. (This zone can be further divided, for larger organizations.) |
| Confidential Payment Card Zone | Mastercard, VISA, American Express | This zone hosts our credit card point-of-sale machines (when not stored in our database). |
| Privileged employee zone | Wired employees | This zone hosts our wired/fixed employee computer terminals. (This zone can be further divided, for larger organizations.) |

### Step 4: Define Controls

Security controls will help to protect the data to the desired sensitivity level. Major areas of controls relate to Authentication/Nonrepudiation: assuring the user is who they claim they are; Confidentiality: making info available only to authorized persons; Integrity: assuring changes are legitimate; and Anti-Hacker: controlling unauthorized access. Specific controls are listed in Table 3.2.4 Network Controls.

Table 3.2.4 Network Controls

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication** | **Confidentiality** | **Integrity** | **Anti-Hacker Controls** |
| Centralized access control (RADIUS, Kerberos, TACACS) | Secret key encryption (AES, 3DES, IDEA, RC4) | Hashing algorithms (SHA-3, HMAC) | Firewall, Unified Threat Management |
| Multifactor authentication (biometric, token) | Public key encryption (Diffie-Hellman, RSA, El Gamal, Elliptic Curve) | Virtual Private Network (IPsec) | Application firewall (web, database) |
| Public key infrastructure | Secure applications: (HTTPS, SSH, SSL/TLS, PGP) |  | Antivirus (endpoint security, email security mgmt) |
| Digital signature | Kerberos: for Authentication & Encryption |  | Log management (SIEM) |
|  | Virtual Private Network (IPsec, PPTP) |  | Vulnerability assessment tools (honeypot) |
|  | Wi-Fi Protected Access (WPA3) |  | Mobile security mgmt. |
|  |  |  | Intrusion Detection Systems (NIDS/NIPS, HIDS/HIPS) |
|  |  |  | Database (Incident tracking, risk/policy management) |

**Action**: In Table 3.2.5, first define which Servers (physical or virtual) are in each of your Zones, and which Services are on each Server. Include one row per Server. Next define the required Controls from the above table, such as encryption, authentication (passwords), hashing, and virtual private network. An IT professional should configure the firewall/router based on this table.

Table 3.2.5: Controls for Services

|  |  |  |  |
| --- | --- | --- | --- |
| **Zone** | **Server**  (\*=Virtual) | **Service** | **Required Controls**  (Conf., Integrity, Auth., Nonrepud., with tools: e.g., Encryption/VPN, hashing, IPS) |
| Internet  (External) |  |  |  |
| De-Militarized Zone |  | Web,  Email,  DNS |  |
| Wireless Network |  | Wireless local employees |  |
| Privileged Server Zone |  |  |  |
| Confidential Payment Card Zone |  | Mastercard, VISA,  Am. Express  Point-of-sale |  |
| Privileged employee zone |  | Wired employees |  |

### Step 5: Draw the Network Diagram

**Path of Logical Access**: A diagram of the networks shows where transactions can enter the system, where they are security-controlled, and where they are processed. Logical paths of entry (Internet, dial-up, wireless, or internal), required controls, and application servers are defined in Table 4.2.1 and 4.2.5. The network is diagrammed, showing firewalls (or border routers), WLANs, servers etc., to ensure Defense in Depth is provided. Text describes logical paths of access (transaction originations and destinations) that help to determine what should flow through routers/firewalls. This will help to define which ports should remain open in the firewall between network zones.

**Action: Network Diagram:** Diagram the network to ensure adequate controls are in place. Show separated or combined servers. Use associated text to define logical paths of access. Servers are colored according to their sensitivity class:

* Green: Public
* Yellow: Privileged
* Red: Confidential
* Purple: Proprietary

**Associated Text**: Once the diagram and Table 3.2.3 is complete, it is helpful to describe in text the various regions of the network, what service connections can go into and out of each region, what transmissions need to be encrypted, and if specific IP addresses can be filtered.

Section 5 includes the firewall and router configurations. Professional network administration personnel should assist in configuring network equipment (firewall, routers) and virtual machines/servers, according to the requirements established in this chapter, and for ensuring additional network security, as defined in Section 5.

## Designing Physical Security

The Physical Security Plan is concerned with physical assets and their protection. The basic concern is what data (or computers) should be physically separated from people and how will this separation be enforced and controlled? If your organization has ATMs or Point of Sale devices, great attention should be spent to physically securing them.

The first step is to understand what assets are stored or available in each room.

### Step 1: Inventory Assets within Rooms

Assets are things of value, and may include computer devices, equipment, and/or files, or non-computer devices, equipment, paper files – or other things of value: money, checks, art, ideas on boards. The first step is to describe the value of what is in each room and the purpose of the room and the assets.

**Action:** In Table 3.3.1, define the purpose of a room, inventory its assets (e.g., devices, information) by room, and define the highest Sensitivity and Criticality Class for the assets contained within it.

Table 3.3.1: Allocation of Assets

|  |  |  |  |
| --- | --- | --- | --- |
| **Room** | **Purpose of Room** | **Sensitivity & Criticality Class** | **Sensitive Assets or Information** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Step 2: Selecting Controls for Sensitivity Classes

Computer equipment must have an adequate environment, and sensitive information must have physical access controls. Rooms are categorized according to the class of data they contain. Site(s) must be diagramed to ensure adequate security.

**Action**: Modify Table 3.3.2 for your organization, to classify how rooms should be treated by the sensitive information they contain (i.e., controls for confidentiality). See section 3.1.1 for Data Sensitivity Classifications. Special Treatment should be organization-specific.

Table 3.3.2: Room Sensitivity Classification Controls

|  |  |  |
| --- | --- | --- |
| **Sensitivity**  **Classification** | **Description** | **Special Treatment** |
| Proprietary | Room contains Propriety information storage. | All cabinets remained locked.  Room remains locked when not attended. No visitors are allowed in these areas. |
| Confidential | Room contains Confidential information storage. |  |
| Privileged | Room contains computer with access to sensitive data or room contains controlled substances. |  |
| Public | The public is free to spend time in this room, without escort. | Unlocked rooms are periodically monitored by guards on a per shift basis.  Specific rooms may be locked during evening/night hours. |

For each room, describe the assets or files that contain sensitive information.

* Access controls include physical, technical, and administrative controls.
* Building entry guards: Obvious main entry, sidewalks, public benches, lighting, low shrubs, few trees, guards, locked doors.
* Room entry guards: Walls, security camera, motion sensor, security alarm, guard or patrol, escorted visitors, employee badges, deadman doors, reinforced windows, and locks: combination, key card, key, biometric.
* Computer access guards: Encrypted disk drive(s), encrypted copier, cable and lock, engraved serial number, disabled disk, disabled USB/disk interface, computer theft recovery software.
* Computer entry guards: Passwords, monitor hoods or privacy monitors, password-protected screensavers, imaged computers, monitor visibility.
* Other: Paper shredder, clean desk, locked files.

### Step 3: Selecting Controls for Criticality Classes

These controls raise availability:

**Power Protection systems**:

* Surge Protector: Eliminates electrical spikes, sags, and surges for fractions of a second.
* Universal Power Supply (UPS): Provides electrical power for up to 30 minutes
* Alternate Power Generation: Can generate electricity for extended periods

**Fire Protection systems**: Smoke detector, manual fire alarm, fire extinguisher, fire suppression system, emergency power-off switch, fire-resistant walls/floors/ceilings, electrical panel, fire department inspects room annually.

**Computer Protection systems**: This section was mostly covered in the Business Continuity section.

* Spare computer, laptop, and/or server.
* Redundant Array of Independent Disk (RAID): survives a single disk failure.
* Redundant networking: Wired and wireless networks
* Redundant site

**Other availability controls**: Air conditioning, water-detection systems.

**Action**: Modify Table 3.3.3 for your organization, to classify how rooms should be treated by the critical information they contain (i.e., related to availability).

Table 3.3.3: Room Criticality Classification Controls

|  |  |  |
| --- | --- | --- |
| **Criticality**  **Classification** | **Classifications related to Availability** | **Controls related to Availability** |
| Critical | Room contains Critical computing resources, which cannot be performed manually. |  |
| Vital | Room contains Vital computing resources, which can be performed manually for a short time. |  |

### Step 4: Complete the Physical Security Map

**Action:**  Draw a layout of the facilities. Show the zoning of rooms including Criticality and Sensitivity Classifications.

**Sensitivity Classification Color Key:**

* Green: Public
* Yellow or Orange: Privileged
* Red: Confidential
* Purple: Proprietary

Alternatively, use shades of white, gray, and black to show increased security. This is helpful for people who have issues seeing colors.

Section 5 includes a table for IT inventory. Professional system administrators may be helpful in installing the access and availability controls, as defined above.

## Attending to Information Privacy

### Step 1: Defining a Data Dictionary with Primary Purpose

The first step is to understand what data an organization has (or needs) and how and why it is used. This is also important in performing a Privacy Impact Assessment (PIA) and classifying information. Data is classified as part of the Information Security chapter, but now we will extend (and potentially update) that table to add a primary purpose and other fields.

A proper **data inventory** describes the types of personal data collected as well as compliance requirements. To start that list, remember that information is generally retained in databases, but could be within documents, spreadsheets or other files.

*Life cycle*: when created; last need: How data is generated and used; when it can be destroyed.

*Format*: Format of file (e.g., pdf, word, excel, mp3)

*Classification, rights, restrictions*: sensitivity and criticality classification; who has access to the data; how the data is protected.

**Action**: Selecting a high priority department with high-risk information, complete a data inventory of databases, records or documents using Table 3.4.1. (Eventually you will want to do this for all departments containing PII.)

Table 3.4.1: Data Inventory

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Department(s)** |  | | | |
| **Location** |  | | | |
| **Data Owner** |  | | | |
| **Data Title** | **Purpose, Description** | **Life cycle**  **When created; last need** | **Format** | **Classification, Rights, Restrictions** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Databases provide a data dictionary showing which fields are within specific records. For paper documents or files, a data dictionary is not available.

**Action**: Manually report paper- or file-based PII in Table 3.4.2.

Table 3.4.2: Data Dictionary for Documents

|  |  |
| --- | --- |
| **Form/Report** | **Data Attributes** |
|  |  |
|  |  |

### Step 2: Performing a Privacy Impact Assessment

This step follows a slightly modified version of the E.U.’s GDPR recommendation.

**Action**: Complete Table 3.4.3 for information that is or should be protected by privacy policy or law.

Table 3.4.3: A Modified GDPR Data Privacy Impact Analysis (part 1)

|  |  |
| --- | --- |
| **Information Type:** |  |
| **Primary Purpose**: What is the primary purpose of processing this data? What are the benefits of the processing – for your organization, and more broadly? What is the intended effect on data subjects? |  |
| **Processing of Data**: How will you collect, use, store and delete data and how will your organization process the data? What is the source of the data? Will you be sharing data with anyone? It is helpful to include a flow diagram of some sort. What data processing may be high risk? |  |
| **Scope of processing**: what is the nature of the data, and which special categories of people or PII does this affect? How many individuals are affected? What data items will you be collecting and using? How often? How long will you retain data? What geographical area does it cover? |  |
| **Context of processing**: what relationship do you have with the individuals? How much control will they have? What is your agreement with the individuals as to how they can access or control their data? What security or privacy issues have you encountered previously? What issues might be of public concern today? What controls do you implement, and how do they relate to current technology? Are you following any approved code of conduct or certification scheme? |  |
| **Consultation with Stakeholders**: How and when will you seek data subjects’ and others’ views – or justify why it’s not appropriate to do so. Who is involved within your organization – including security or other experts? |  |
| **Privacy Principles:** How will privacy principles be addressed? If you address specific regulation, how are specific articles met? How will you prevent function creep and update and maintain policy implementation? |  |

In a privacy impact analysis, the threats must be evaluated from the perspective of the data subject (generally, client). Table 3.6.4 is the traditional risk analysis applied to privacy and security.

**Action**: Identify privacy and security risks as part of Table 3.6.4. The type of privacy issues (e.g., breach, stigmatization, de-identification, surveillance, inaccurate data) should be recorded.

Table 3.4.4: Risk Analysis Component of PIA

|  |  |  |  |
| --- | --- | --- | --- |
| **Source of risk and impact on individuals** | **Severity**  **(Minimal, significant or severe)** | **Likelihood**  **(Remote, possible or probable)** | **Overall Risk**  **(Low, medium or high)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Action**: Once the threats are documented, design controls to reduce or eliminate threats.

Table 3.4.5: Controls to Reduce Privacy Risk

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | **Optional controls to reduce or eliminate risk** | **Effect on risk**  **(eliminated, reduced accepted)** | **Residual risk**  **(low-medium-high)** | **Measure approved**  **(yes/no)** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Step 3: Developing a Policy and Notice of Privacy Practices

Next comes the job of building transparency and trustworthiness via a clear communication with employees and data subjects, indicating how data subject information will be used, and possibly, how they can access and petition to amend their data. Two documents commonly adopted for communicating information privacy policy to data subjects include [CDPSE20]:

**Notice of Privacy Practices (NPP):** This is a record to the outside world describing how the controller obtains and uses data. Data subjects and government authorities are the indented audience.

**Consent Form:** After reading the NPP, the data subject is expected to sign a consent form, indicating that the data subject is aware of how their personal information will be used.

In addition, internal employees must also be aware of how privacy will be implemented in the organization, through policy documentation and training. Privacy Policies are internal documents used to communicate rules to employees describing how personal information is to be handled. They are followed up with procedures, standards and guidelines, as described in the Governance chapter.

**Action**: Development of the Notice of Privacy Practices means answering the questions in the following table. To complete the table, perform the following:

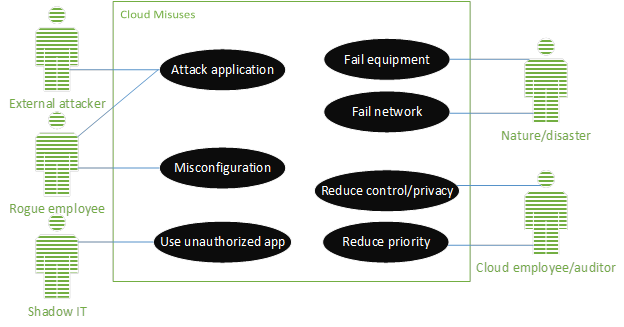
1. What does the regulation your organization must adhere to say? What might your lawyer recommend?
2. What might you learn from other organizations?
3. What will work with different your organization? What privileges might your data subjects prefer?
4. Consider how you will communicate your NPP, including posting the NPP on website, office walls, contracts, customer forms.

Table 3.4.6: Notice of Privacy Practice

|  |  |
| --- | --- |
| **Notice of Privacy Practice** | |
| What data is collected? |  |
| To whom is data shared? |  |
| How long is data retained? |  |
| What rights do data subjects have to inspect and change their records? |  |
| How can data subjects inspect and amend their records? |  |
| How will the NPP be made available to data subjects? Is a consent form required, and if so, how is it obtained? |  |

## Managing Cloud Security

This section will help to decide contractual issues that are a concern when signing contracts with cloud providers. First consider the threats that can occur within the cloud.



### Step 1: Define Security and Compliance Requirements

***Action***: First, review security, privacy, and regulatory threats related to the application that you want to move to the cloud. Then complete the table outlining your concerns as notes.

Table 3.5.1 Define Security, Privacy and Compliance Requirements

|  |
| --- |
| **Confidentiality Concerns**  (two examples provided)  **Security issue**: Cloud employee sells personally identifiable information related to ….  **Privacy issue**: Medical data is released, embarrassing client; may affect their job, career. |
| **Integrity Concerns** |
| **Availability Concerns** |
| **Regulatory Concerns** |

### Step 2: Select a Cloud Provider and Service/Deployment Model

**Action**: For each of the categories of questions below, consider which areas might be a concern for your organization in your adaptation of cloud services. This will define what you are looking for in the Service Level Agreement (SLA), which serves as a contract between you and the cloud provider. What are priorities, and required versus desired features? Use the Information Security Data Classification Tables and Handling of Sensitive Data Table to help complete this section.

#### Regulatory issues

|  |  |
| --- | --- |
| **Questions** | **Notes** |
| What do my nation’s laws require in protecting my data? What international laws, data privacy laws and state breach laws are my data subject to? |  |
| Where (e.g., which country) will my client data reside, and what government intrusion, security and privacy laws might my data be subject to? What is cloud provider policy if law enforcement subpoenas a client’s sensitive information? |  |
| What cloud controls are in place to address these regulations? How will breaches be notified and handled? (Ultimately the cloud customer is responsible for security) |  |
| What are cloud provider privacy policies related to client data? What security controls and monitoring are provided for the client? |  |

#### Cloud Provider Security Implementation

|  |  |
| --- | --- |
| **Questions** | **Notes** |
| What controls are implemented by the cloud provider for confidentiality, integrity and availability, or more specifically, authentication, access control, digital certificate exchange, IDS, trusted platform? What network security controls exist? |  |
| What policies and security implementations prevent cloud personnel from accessing and leaking client data? |  |
| What third-party audit processes exist? What does the audit involve and how are results disseminated? How often are audit/compliance results provided? What have previous audit results shown? |  |
| Does the cloud provider maintain and publish metrics on availability (or downtime)? |  |
| What cloud tools are available for testing and monitoring of security? What protocol and restrictions exist for the cloud user to perform vulnerability and penetration testing? |  |
| What types of alarm/logs does the cloud provider monitor for? Are client-system logs available to clients? |  |
| Can clients monitor the usage and access of their data? |  |

#### Cloud Incident and Disaster Recovery

|  |  |
| --- | --- |
| **Questions** | **Notes** |
| What rates of availability does the cloud provider maintain? Can data be maintained redundantly in multiple regions? How is data synchronization achieved? Can the organization’s recovery point objectives and recovery time objectives be achieved? |  |
| What are the cloud server provider policies for disaster recovery? How does the cloud provider handle disaster recovery? What is included in the contractual agreements? |  |
| How is incident response handled by the cloud provider? What tools are available to clients to forensically analyze incidents? |  |

#### Contractual Issues – Cloud Provider and Third Party

|  |  |
| --- | --- |
| **Questions** | **Notes** |
| What is the cloud provider standard Service Level Agreement? Can this SLA be personalized for my needs? |  |
| If we are under contract to another organization, does the proposed cloud implementation meet our contracts’ requirements? What issues does our contract specify or imply? |  |
| What happens at contract termination? What are the cloud provider’s data privacy policies? How does data export to another system work, what is this cost, and what are cloud provider policies for data destruction? |  |
| Is the cloud provider reputable, financially stable, protected by insurance, located primarily (or entirely) in the home country? What recent legal cases have involved the cloud provider? (casetext.com can provide details.) |  |
| What security APIs or form interfaces are supported to automatically configure a security configuration? Does the cloud provider support the API required by the client? What kind of scripting and key management options does the cloud provider provide? |  |

Further stages are beyond what can easily be accomplished in a classroom environment and thus are not fully defined as part of the workbook. They include:

### Step 3: Define architecture

This stage is beyond the scope of the book. It involves selecting cloud deployment model: e.g., IaaS, PaaS, SaaS, DaaS, virtualization, multicloud configurations and more detailed configurations

### Step 4: Assess shared security responsibility: your’s & cloud’s

This involves completing a list of controls provided by each.

**Action**: Consider how and who will provide security for each layer, adding notes to the diagram below.

### Step 5: Monitor and manage changes

**Question**: Which metrics will be available to you to monitor in the cloud? You will want to monitor usage, attacks, defenses, software update monitoring, backups, etc. (See chapter on Metrics for additional ideas).

## Organizing Personnel Security

Personnel and customers are both a potential weakness in the security defense system, as well as a potential source of fraud. Many of these threats would be industry specific. For example, a bank would be susceptible to the sale of credit card numbers, and creation of fake accounts with transferred money.

### Step 1: Controlling Employee Threats

**Action:** In Table 3.6.1, list threats to services that could be subverted, and by whom. List threats (can be from Risk section and you may consider new ones.) An example threat might be: ‘unreported sales’ by ‘salesperson’ resulting in ‘theft and incorrect inventory’.

Table 3.6.1: Defining Personnel Threats

|  |  |  |
| --- | --- | --- |
| **Threat** | **Role** | **Liability or Cost if Threat Occurs** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

The following controls can help to prevent fraud from occurring:

* **Security Responsibility**: A Chief Information Security Officer (CISO) makes someone responsible for security. Other security roles include: Data Owner, Process Owner, Info Security Steering Committee, Incident Response Management/Team, Security Analyst, Security Administrator.
* **Segregation of Duties**: No one person can subvert the system. Includes authorization forms and access control.
* **Security awareness training**: Discussion of organization policies, legal compliance, appropriate password selection, appropriate use of computer, recognizing and reporting security events. Security training and education train certain roles for specific security responsibilities.
* **Training and written policies and procedures**: Appropriate skills and knowledge of standards to do job.
* **Signed agreements**: Can list job responsibilities. Privacy Policy describes confidentiality agreement, security requirements. Acceptable Use Agreement defines proper computer use, including email. Other agreements: Code of Conduct, Service Level Agreements.
* **Background checks**: Background checks are important for any employee who handles protected individual information (PII), including system and security administrators.
* **Need to Know/Least Privilege**: As per information security, minimal access to information.
* **Ethical culture**: Management must live, mentor and insist on ethical behavior.
* **Employee Support Program**: Program assists employees in personal or financial trouble.

Detective Controls include:

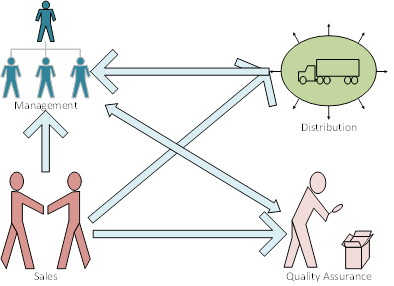
* **Fraud reporting mechanism**: Customers and employees can discreetly report potential fraud to independent agent.
* **Transaction Logs**: Some transactions should be logged, providing the potential for review.
* **ID Badges**: Distinguish between onsite employees, contractors and visitors.
* **Internal Audit**: Planned and surprise audits detect and deter fraud.
* **Mandatory vacations or job rotation**: Inappropriate performance is eventually recognized, when segregation of duties is not possible.

Corrective Controls include:

* **Employee Bonding, Fidelity Insurance**: Insurance protects against losses due to theft, mistakes and neglect. (This is illegal in some countries.)

Segregation of Duties requires a more extensive explanation. Good management ensures that no one person can defraud the system. Roles are categorized into Origination, Authorization, Verification, and Distribution, which originate, approve, double-check, and act on, respectively. If this is not possible to attain due to organization size, job rotation and mandatory vacations are compensatory controls.

Figure 3.6.1: Segregation of Duties



**Action**: Now consider how each of the threats can be controlled in the following table.

Table 3.6.2: Defining Personnel Controls

|  |  |  |
| --- | --- | --- |
| **Threat** | **Role** | **Control** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Step 2: Allocating Responsibility to Roles

What security implementation is each role responsible for? The controls above are one concern. However, other concerns may be in effect for each area of security: policies, risk, business continuity, information security, network security, physical security, incident response, personnel security, and metrics. Look up the sections to determine proper training for the staff. Often one person is allocated as the Chief Info Security Officer. (This is required by HIPAA.)

**Action**: Complete 3.6.3 by adding responsibilities to roles, and also adding new roles and responsibilities, as needed. It may be useful to specify a name next to a role, too, for small organizations.

Table 3.6.3: Responsibility of Security to Roles

|  |  |
| --- | --- |
| **Role** | **Responsibility** |
| Chief Info Security Officer | Lead Info Sec. Steering Committee and incident response teams.  Lead efforts to develop security policy, security workbook.  Manage security projects, budgets, staff.  Lead security training for required staff on PCI DSS, ...  Maintain security program: metrics, risk, testing, and policy revisions. |
| Personnel | Participate in Information Security Steering Committee.  Tracks and documents theft (to determine pattern).  Prepare/manage contracts with Third Party contracts, establishing expectations relative to security.  At hiring: Perform background check for persons handling confidential info/major assets. Write job description considering segregation of duties, security responsibilities.  For each employee:   * Signs Acceptable Use Policy; * Takes security awareness training including compliance, policy training   At termination: Revoke computer authorization, return badges/keys and equipment, notify appropriate staff. |
| Security Admin | Monitor logs for secure systems daily  Enable/disable permissions according to data owner’s directions  Configure security appliances; audit equipment  Rebuild computers after malware infection  Investigate incident response, collect security metrics as part of Incident Response Team. |
|  |  |
|  |  |

### Step 3: Define Training, Documentation and Tools to Manage Security

Consider the following tools to manage security:

* Code of Conduct: High level policy relating to general employee behavior
* Acceptable Use Policy: Detailed policy defining computer responsibilities
* Configuration Management: Tracks software versions and other configurations
* Change Control: Tracks change requests, relating to defects, fixes and other transactions
* Service Level Agreements: Contracts with service providers.

**Action**: What tools, training and written procedures are necessary for each role? For training, consider which training is required at hiring and ongoing.

Table 3.6.4: Requirements for Security Roles: Training and Documentation

|  |  |
| --- | --- |
| **Role** | **Requirements: Training, Documentation, Tools** |
| Chief Info Security Officer | Training:   * Security certification required at hiring. * Annual security maintenance training:   Documentation:   * Development of Security Workbook, legal compliance checklist |
| Security Administrator | Training:   * Security certification required at hiring. * Annual security maintenance training:   Documentation: TBD |
|  |  |
|  |  |

Remember to look into requirements for specific regulations your industry must adhere to.

## Planning for Incident Response

Incident response is concerned with what should happen when an organization’s systems have been or may have been compromised. Potential responses include closing the external network (and its services) down, leaving the network up but investigating the attack, bringing the system down, etc. The actual response is best determined by executive management, and their decisions will vary depending on the type of organization (e.g., bank, Web search engine, medical establishment, etc.) What needs to be considered in advance is how the system administrator should react, who should be notified, what approach the organization will take in relation to an investigation, etc.

The stages of Incident Response include:

**Step 1: Preparation:** Plan before the attack

**Step 2: Identification**: recognition of attack

* prioritize the symptoms to go after first.

**Step 3: Containment**: the attacker cannot proceed further

* you have halted but not cleared the attack.

**Step 4: Analysis and Eradication**: The network is cleared of the attack

* you have found the root cause: what enabled the attacker entry into network

**Step 5: Recovery**: retest system and restore normal operations

**Step 6: Lessons Learned**: review what happened;

* how can you improve next time?

In the workbook, we prepare for incident response, thus accomplishing Step 1. However, planning for the other steps all occur in this Step 1, so consider all stages in your design.

### Step 1A: Determine types of concerning attacks and how they will be detected

This involves the following steps:

1. Consider whether the incidents listed in table 3.7.1 apply to your organization. Add or subtract incidents as you see fit for your organization.
2. Consider the best ways of detecting these incidents. What technologies, training, and procedures should be in place to detect these incidents? Add them to the table. Consider the following technologies: computer logs, alarms, and error messages, antivirus software, security training, audits, penetration and vulnerability tests, system baselines, network sniffing, network or host intrusion detection systems.
3. What is the appropriate handling of each incident? Consider these questions: If you know an intruder is in your network, should you bring down the network, or leave it up? Should law enforcement be called? Who should be notified, and how, for which types of attacks? The CEO or President should be deciding the answers.

If the procedure can be concisely described in Table 3.7.1, specify in the Procedural Response column. If an extended procedure is included, complete a copy of Table 3.7.2 to define the Incident Handling Response Overview details. Then refer to this new table in the Table 3.7.1 Procedural Response column.

If prosecution is to be considered, law enforcement will need to be called at an early stage to ensure that all evidence is properly handled and chain of custody is adhered to.

**Action**: Complete Table 3.7.1 as per the above directions. You may add specific attack types as necessary for your organization.

Table 3.7.1: Table of Incident Types

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident** | **Description** | **Methods of Detection** | **Procedural Response** |
| Intruder accesses internal network | Firewall, database, IDS, or server log indicates a probable intrusion. (May qualify as espionage.) |  |  |
| Break-in, loss or theft | A laptop, backup tape, or memory source with confidential information was lost or stolen. |  |  |
| Social Engineering | Suspicious social engineering attempt was recognized OR information was divulged that was recognized after the fact as being inappropriate. |  |  |
| DDOS | Server or network approaches 85% or higher utilization |  |  |
| Trojan Wireless LAN | A new WLAN masquerades as us. |  |  |
| Data Breach | Inappropriate access to proprietary or confidential information |  |  |
| Violation of Policy | Violation of organizational standards and rules:  Unauthorized access or changes to IT, information, or service |  |  |
| Malware | Antivirus software reports malware, whether or not it can be automatically cleaned;  Employee reports unusual behavior |  |  |
| Ransomware | Criminals infiltrate and encrypt our servers, ask for ransom to decrypt and not publish data |  |  |
| Surveillance/ Espionage | An external party infiltrates the organization in order to steal proprietary information. |  |  |

### Step 1B: Design the Incident Response Handling Forms

**Action**: Complete a copy of Table 3.7.2 Incident Handling Response Overview for each incident type requiring an extended explanation. The fields of the table shall be completed as follows:

* **Contact List**: All persons who should immediately be contacted should be listed here.
* **Emergency Triage Procedure**: List of steps or name of a procedure file that is to be executed by anyone on staff at the time of the incident.
* **Containment & Escalation Conditions and Steps**: Steps or procedures to contain the threat and notifications that should occur if certain conditions arise during the Triage Procedure (e.g., inordinate delays, further events, etc.)
* **Analysis, and Eradication**: The procedure to analyze the root cause and recover the system to normal. The roles or persons responsible for performing this procedure are named. For example, this may mean IT admins rebuild the system after a virus is found.
* **Other Notes**: This may include notes explaining the reasons for certain actions, special conditions, or associated prevention techniques.

Table 3.7.2: Incident Handling Response Overview

|  |
| --- |
| **Incident Type:** |
| **Contact Name & Information:** |
| **Emergency Triage Procedure:** |
| **Containment & Escalation Conditions and Steps:** |
| **Analysis & Eradication Procedure:** |
| **Other Notes (Prevention techniques):** |

**When Incident Occurs:** Complete the Incident Response Report when an incident occurs. An Incident Report is included as Appendix A. This report is to be completed for each incident. This report is for internal use only – law enforcement should be contacted at early stages if legal proceedings may be desired.

If there are extended incident response procedures, they should be included in Section 5 Business Continuity. A competent system administrator can help ensure that the detailed procedures affecting IT are functional.

## Defining Security Metrics

### Approach 1: Implementing Business-Driven Metrics

Metrics are part of the Monitoring and Compliance function, and help to indicate whether controls and compliance are effective or not. While metrics are not absolutely necessary for the average small organization, any organization that is subject to regulation (e.g., HIPAA, SOX, FISMA) should take this section very seriously. In fact, most organizations would benefit from a few carefully selected metrics.

Strategic metrics include risk (ALE), budget, disaster recovery test results, and regulatory compliance.

Tactical metrics include policy compliance/non-compliance, incident management effectiveness, and risk changes resulting from system changes.

Operational metrics include firewall, IDS, or system log analysis, vulnerability test results, patch management status.

Here are some sample metrics, which may or may not apply to your organization.

***Table 3.8.1: Example Metrics***

|  |  |
| --- | --- |
| Risk:  The aggregate ALE  % of risk eliminated, mitigated, transferred  # of open risks due to inaction | Cost Effectiveness:  Cost of workstation security per user  Cost of email spam and virus protection per mailbox |
| Operational Performance:  Time to detect and contain incidents  Quantity & severity of incidents  % of systems audited in last quarter | Organizational Awareness:  % of employees passing quiz, after training vs. 3 months later  % of employees taking training |
| Technical Security Architecture:  # of malware identified and neutralized  Types of compromises, by severity & attack type  Attack attempts repelled by control devices  Volume of messages, KB processed by communications control devices | Security Process Monitoring:  Last date and type of BCP, DRP, IRP testing  Last date asset inventories were reviewed & updated  Frequency of executive management review activities compared to planned |
| Security Management Framework:  Completeness and clarity of security documentation  Inclusion of security in each project plan  Rate of issue recurrence | Compliance:  Rate of compliance with regulation or policy  Rate of automation of compliance tests  Frequency of compliance testing |
| Secure Software Development:  Rate of projects passing compliance audits  Percent of development staff certified in security  Rate of teams reporting code reviews on high-risk code in past 6 months | Incident Response Metrics:  # of Reported Incidents  # of Detected Incidents  Average time to respond to incident  Average time to resolve an incident  Total number of incidents successfully resolved  Total damage from reported or detected incidents  Total damage if incidents had not been contained in a timely manner |

**Action**: Complete Step 1, Step 2, and Step 3 questions below.

**Step 1 Question**. What are the most important areas to monitor in your organization? What threats and legislation are you most concerned with? You may want to review risk and policies to help define the most important areas to monitor.

**Step 2 Question**. After listing the most important threats, consider which metrics make the most sense to collect. Since automated metrics are doable in a busy world, is there an easy way to collect these metrics?

**Step 3 Question**. Consider the following three perspectives and different audiences:

* **Strategic**: Management level: audit, policy; may discuss annually.
* **Tactical:** Observe how you are performing; view trends; may discuss every six months.
* **Operational**: Gather metrics and look at them; may discuss weekly or monthly.

**Action**: After considering these three questions, complete Table 3.5.2 below:

***Table 3.8.2: Selected Metrics***

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Metric** | **Calculation and Collection Method** | **Period of Reporting** |
| Strategic |  |  |  |
|  |  |  |
| Tactical |  |  |  |
|  |  |  |
|  |  |  |
| Operational |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

### Approach 2: Implementing Technology-Driven Metrics

Recognizing that it is not possible to build a secure network in a day, prioritize three to implement next, knowing that all should be implemented, and potentially assuming some already are. Below, justify why these 3 metrics are important to your business to prioritize in implementation. Refer to the book or slides for information on each of these metrics and tools.

1. Inventory of Authorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Management of Protected and Sensitive Data
4. Secure Configurations for Hardware and Software
5. Account Monitoring and Control
6. Controlled Access Based on Need to Know
7. Continuous Vulnerability Assessment and Remediation
8. Management of Audit Logs
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery Capability
12. Secure Configurations for Network Devices
13. Network Attack and Log Monitoring
14. Security Awareness Skills Training
15. Management of Service Providers
16. Application Software Security
17. Incident Response and Management
18. Penetration Testing

It may be useful to iterate through the metrics, selecting the top 3 metrics, then quarterly adding 3 additional metrics. A competent system administrator or programmers can help to automate the collection of computer-generated metrics.

**Action Question: Describe your three priority metrics sections to add with justification here:**

## Planning to Gather Forensic Information

Forensic analysis includes three aspects that occur simultaneously:

* Forensic analysis: high level skills of asking what, when, who, where, how, why?
* Technical forensic abilities: methods to collect evidence
* Legal perspective: establishing chain of custody

### Aspect 1 Forensic Analysis: Establishing Forensic Questions

The first stage is to ask the right questions in order to determine the total impact and scope of the incident. These questions will lead the investigation. Use table 3.9.1 to outline specific questions that apply to an incident. The questions provided should only give ideas as to what you might ask.

**Action**: Prepare a list of questions that should be investigated for a named incident that is a threat of concern at your organization.

*Table 3.9.1 Questions for Investigation: Who, What, When, Where, Why, How…?*

|  |  |
| --- | --- |
| Incident |  |
| Date |  |
| Questions to Investigate | When was the incident detected and how?  Who was impacted by it?  Who introduced it and why?  How do we eliminate the threat?  What information may have been compromised?  What else might have occurred as part of this incident? |

### Aspect 2 Technical Perspective: Methods to Collect Evidence

Evidence can be found across the network and in host client and server machines:

* Collect volatile information: collect the current picture of what is happening (via jumpkit)
* Collect and analyze logs and information from various network and host devices;
* Copy and analyze disk images

A discussion of logs and some commands to collect volatile information are included in the text. Table 3.9.2 provides an overview of information that may be accessible on your network’s devices.

**Action**: Edit Table 3.9.2 with forensic information accessible on your network devices. You may want to indicate which specific commands and/or logs provide the required information.

Table 3.9.2 Collecting important technical information

|  |  |  |
| --- | --- | --- |
| **Source** | **Security Information** | **Sample attacks** |
| Router | Reverse IP address, statistics, illegal packets | IP spoofing, DDOS, formatting errors (e.g., LAND, teardrop), footprinting/nmap, illegal destination IP or port numbers |
| Firewall | Prohibited packets for covered protocols, statistics | DDOS/flooding, amplification attacks, formatting errors, fragmentation attacks, exfiltration |
| DNS | Track who accessed services when (email, web, ssh) | Inappropriate websites, DNS downloads |
| Application Server | View abnormal and abusive events, and potentially view completed events | Formatting errors, encoding attacks,  SQL attacks |
| Authentication Server | Successful/unsuccessful login, unusual times | Password attacks (dictionary, brute force), impersonation |
| Switch | Translate MAC address to physical port | MAC spoofing |
| Wireless Access Point | Identify (inappropriate) MAC address | Rogue WAP, MAC spoofing |
| Web Proxy | Track web accesses, cache status of web accesses | Malware origins, inappropriate web accesses |
| Intrusion Detection | Track specific application attacks | Nmap, encoding attacks |
| All Devices | Configuration changes, cleared logs, login | Hiding tracks, enabling backdoors, password attacks |

### Aspect 3 Legal Forensics: Ensuring Chain-of-Custody

Digital Evidence form describes a piece of evidence, including:

* Timeline: where/when it was collected, stored and imaged
* Witnesses to transactions
* Evidence description: includes manufacturer, model, serial number, and digital hashes.
* Cryptographic hashes: ensure that the forensic artifacts are not modified.
* Evidence is stored in evidence bags, sealed with evidence tape, and stored in locked cabinets in a secured room.

A Chain of Custody form tracks who handled the evidence from minute to minute and ensures that the evidence was properly sealed and locked away with extremely limited access. The Chain of Custody document describes:

* when and where the evidence was held/stored, and
* the name, title, contact information and signature for each person who held or had access to the evidence at every time point and why they had access

# Performing an Audit

This workbook provides audit standards to help small organizations perform their own internal audits. Risk-based auditing considers what parts of the organization should be audited with highest priority, and plans those audits first. An audit plan and a report outline are shown, and then example specific audits are included.

Vocabulary to review includes:

**Inherent Risk**: Susceptibility to a problem (e.g., a bank’s inherent risk is a thief)

**Control Risk**: A problem exists that will not be detected by an internal control system. For bank: A thief accesses another’s account at Money Machine but is not detected

**Compliance Testing**: Verify that the controls effectively implement security as expected

**Substantive Testing**: Verify that the business applications work as expected – accurately and completely.

Audit tasks may involve:

* **Review IS Organization**: Separation of duties
* **Review IS Policies, Standards, Procedures**: Defined, periodically updated
* **Review IS Documentation**: Policy, Procedures, Design, Test, Operations, Contract/SLAs, Security
* **Interview personnel**: Segregation of duties, security awareness, competency
* **Observe personnel**: Document everything in sufficient detail
* **Investigate actual data**: Use General Audit Software to investigate data (database, logs, reports, etc.)

## Audit Planning

**Action: Consider the answers to the following questions, then complete the Audit Plan table below.**

Risk-based auditing considers what should be tested first. Consider…

* What parts of our business are the most susceptible to risk?
* What regulations must we test for?
* Is this security plan complete and implemented?
* What business/IS systems are changing?
* Are new evaluation tools available?
* Are there new regulations to test for?

Answers may lie in the Risk or BIA sections.

*Table 4.1.1: Audit Planning Table*

|  |  |  |  |
| --- | --- | --- | --- |
| **Audit Area** | **Timeframe** | **Date of Last Test** | **Responsibility** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Audit Engagement Plan Standard

**Action: Complete the formatted audit engagement plan below.**

Table 4.2.1: Audit Engagement Plan

|  |
| --- |
| **Purpose:** <Include basic purpose of audit> |
| **Objective**: <What does the audit want to find out> |
| **Scope**: <Describes constraints of audit> |
| **Compliance and Criteria:** |
| **Constraints**: |
| **Risks:**   * Inherent Risks: (Risks organization is predisposed to) * Control Risks: (Risk that a control has vulnerability(s)) * Detection Risk: (Risks of auditor not detecting a problem) |
| **Approach:** <At a high level, how will the audit test for its objectives?> |
| **Checklist**: <This section should include the bulk of the audit plan. It should include audit setup, audit tools, list of persons to be interviewed, and forms of compliance or substantive testing.> |
| **Signatures:** <Provide names of persons responsible for accepting the audit engagement plan.> |

## Evaluation of Design of Security Controls

The control matrix can help in determining where controls are weakest, and thus where vulnerabilities may exist. These can be listed directly as findings, and can be further tested to determine their specific vulnerabilities.

Attacks or problems are listed as column headings across the top row of the table, while controls are listed as row headings down the left-most column. Attacks and controls can be added as needed.

Controls can be evaluated per vulnerability as Strong (\*\*\*), medium (\*\*), weak (\*), or blank for not applicable/appropriate/available. In addition, controls can be evaluated as Preventive (P), Detective (D), or Corrective (C). It is possible to indicate Strong Preventive as (PPP). It is recommended that at least one strong control exists and multiple controls exist.

**Action**: Evaluate the attacks and controls below, and their applicability to your organization. Update the table as appropriate.

*Table 4.3.3: Evaluation of Design of Internal Controls*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Problem->  Control v | Disk  Failure | Power  Failure | Data  Breach | Fraud | Hack | Malware | Social  Eng. | Stolen/  Lost  Equip. |
| Access Control |  |  | P | p | p | p |  | d |
| Authentication |  |  | pp |  | pp | p |  |  |
| Antivirus |  |  | pp |  |  | pd |  |  |
| Firewall |  |  | d |  | pp | p |  |  |
| Logs/Alarms/SIEM | d | d | pd | c | d | d |  |  |
| Physical security |  |  | P | p |  |  |  | pp |
| Strong policies, standards, guidelines, procedures | cc | cc |  |  |  |  | p |  |
| Security awareness training |  |  |  | d |  | p | ppd | p |
| Vulnerability mgmt. |  | pp | pp | p | d |  |  |  |
| Email security mgmt. |  |  |  |  |  | pd | p |  |
| Application firewall |  |  | dd |  | pd |  |  |  |

## Audit Report Standard

The Audit Report is not part of the audit planning process; it is used to provide results after a completed audit.

**Action**: After completing an audit, complete the Audit Report.

Table 4.3.4 Completing an Audit Report

|  |
| --- |
| **Objective:** (Same as Audit Engagement Plan) |
| **Scope**: (Same as Audit Engagement Plan) |
| **Period of Audit:** |
| **Compliance and Criteria:** (Same as Audit Engagement Plan) |
| **Assertions: <**Management statements as per Engagement Letter or Audit Engagement Plan> |
| **Executive Summary**: <Overall findings, opinion and reservations or qualifications.> |
| **Detailed Findings and Recommendations**: <A detailed description of what was found.  Group by materiality or intended recipient  Mention things done well, faults and constructive corrections  Include expected follow up> |
| **Evidence**: <Where are support results (may be separate)?> |
| **Signed & dated:** <Signed by auditors> |

## Audit Help Guides

This section includes some recommended audit plan questions and tools.

### Equipment Baseline Audit

Equipment audited:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Auditor:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Also present:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Table 5.5.1 Equipment Baseline Audit

|  |  |  |
| --- | --- | --- |
| **Topic** | **Standard** | **Finding** |
| Inventory | Does equipment tag, H/W, S/W match inventory record? |  |
| Antivirus | Last date updated |  |
| Automatically updated |  |
| Result when run |  |
| Password | Password complexity meets standard |  |
| Patching | Automatic patching enabled |  |
| Last date patched |  |
| Minimized Services | Last date internal services were checked/minimized. |  |
| Vulnerability scanner results & date checked |  |
| Minimized Vulnerabilities | Network ports observed by scanner include |  |
| Date of last scan |  |
| Backups | Last full backup taken |  |
| Location backup saved offsite |  |

Some portion of equipment should be monitored annually – servers should be monitored more regularly than employee terminals.

### Audit Questions for Employee Policy Adherence

This section offers some good checks to ensure that employees are aware of policy and their actions adhere to policy.

Audit questions for employees:

Who do you contact when a virus or other malware is found?

Who would you contact if you suspected fraud?

Has anyone ever used your login/password?

Do you have a written job description?

What security and privacy functions do you do as part of your job description?

Is there sufficient training or documentation for you to do your job?

What legislation do you adhere to and how?

Are you happy with your job?

Do you use your work password to login to any other location? What is that password? (They should not provide and if they do, the password should be changed)

Auditor checklist:

Are login/passwords taped to terminal or nearby?

Can the password be guessed based on interests?

Is any confidential information in the office wastebasket?

Do access permissions adhere to authorization records?

# Operational Security Plans

This Operational section is meant to document the required configurations of the security or secured devices, and the procedures to carry out security policies. These are at the lowest level of security detail.

***This section contains a bare-bones minimum security implementation as a start point. Section 5 is beyond the scope of the Security Planning: An Applied Approach book.*** ***Note that both NISTIR 7621 and partial PCI DSS documents that this section was taken from have newer editions and this section is not up-to-date. The material is provided in as-is condition, assuming that a partial implementation may save you time. Please use with extreme care and update according to your own needs.***

The first section of each subsection (6.1 Information Security, 6.3 Network Security, etc.) includes a list of detailed standards for security implementation. The two top priority standards are indicated with a \* and \*\*, and they are considered Absolutely Necessary and Highly Recommended, respectively. They originate from the National Institute of Standards and Technology (NIST) recommendation: Small Business Information Security: The Fundamentals. (Ref: <http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7621-Rev.1>.) Additional information on these recommendations is available at this Web reference. *This section is being updated currently for Rev. 1.* A partial implementation for PCI DSS is provided.

Following the Standards are sections for detailed Procedures. Most of these procedures are for more ‘mature’ organizations to complete after performing Sections 3 and 4 of this workbook. These procedures describe in detail how certain tasks are to be accomplished. These Procedures are necessary to complete the full picture created in Sections 3 and 4 of this workbook.

Each organization should complete the procedures by priority (which may be mandated by specific regulations for the organization.) The organization should continue to add additional security as it matures. More advanced security standards include:

* PCI DSS (<https://www.pcisecuritystandards.org/security_standards/pcidss_agreement.php?association=pcidss>): Full implementation for organizations taking payment cards. Obtain the document: PCI DSS version 3.1 (at time of writing).
* COBIT ([www.isaca.org](http://www.isaca.org)): specifically for corporations
* ISO/IEC 27002:2013: International Standards Organization’s Information technology -- Security techniques -- Code of practice for information security controls (<http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54533>)
* Center for Internet Security: Has *technical* standards for configuration of operating systems, servers, networks and more. See: (<https://benchmarks.cisecurity.org/downloads/benchmarks>)
* NIST Security Control Family (<http://csrc.nist.gov/publications/PubsFL.html>): specifically for organizations dealing with the U.S. government.

## Information Security

The Standards section includes recommendations from NIST that all small businesses should adhere to. Many of the directives can be designed during Tactical security planning, in Section 4.1 Designing Information Security. Mature organizations shall also define a procedure on how to request and allocate computer application privileges.

### Information Security Standards

The following indicates the priority of the recommendations:

Recommendations with 1 asterisk\*= NISTIR 7621 Absolutely Necessary

Recommendations with 2 asterisk\*\*= NISTIR 7621 Highly Recommended

Recommendations with superscript**CC**= PCI DSS partial recommendation

Require individual user accounts for each employee on business computers and for business applications\*

1. Every employee should have an individual login account.
2. Employees should not be logged in as administrator, to avoid harmful actions if the computer is compromised.
3. Passwords should be complex, including a combination of upper/lower case, numbers and punctuation, and at least 12 characters long. Passwords should be changed every 3 months.

Limit employee access to data and information, and limit authority to install software\*/CC

1. When giving access to data, ensure the least privileges are assigned.
2. Provide access to only the system or information required doing a job. This helps to avoid insider abuse.
3. Segregation of duties should be followed while assigning roles and responsibilities. For example, an employee initiating a transaction should not be allowed to approve it as well.
4. To restrict installation of software, ensure employees do not use administrative accounts as normal login.
5. Access to system components and cardholder data should be limited to those individuals whose job requires access.**CC**

Protect stored cardholder dataCC

1. Do not store sensitive data after use (even if encrypted).
2. Do not store the full contents of any track (from magnetic stripe located on the back of card, equivalent data contained on a chip, or elsewhere).
3. Do not store the card verification code or value (three or four digits, printed on the front or back of a payment card).
4. Do not store the personal identification number (PIN) or the encrypted PIN block.
5. Hide the primary account number (PAN) when displaying. The first six or last four digits are the maximum number of digits to be displayed.
6. Never send unprotected primary account numbers (PANs) by end-user message technologies. End-user message technologies include email, instant message, chat, or any other electronic methods.

Assign a unique ID to each person with computer accessCC

1. There should be two-factor authentication for remote access from outside the network including by employees, administrators, and third parties.
2. Enable remote access accounts for vendor(s) only during the time period needed. Monitor remote access account when in use by vendor(s).

### Procedure for Authentication

How are computer system/application permissions requested, approved, and tracked?

## Computer & Server Security

The Standards section includes recommendations from NIST that all small businesses should follow. Mature organizations shall also define how changes are requested and tracked, how software is requested and tracked, and standard terminal configurations.

### Computer/Server Security Standard

The following indicates the priority of the recommendations:

Recommendations with 1 asterisk\*= NISTIR 7621 Absolutely Necessary

Recommendations with 2 asterisk\*\*= NISTIR 7621 Highly Recommended

Recommendation with superscript**CC** = PCI DSS Partial Implementation

Protect information/systems/networks from damage by viruses, spyware, and other malicious code\*/CC

The recommendations to ensure computers in the office network are protected from virus, spyware, and other malicious code include:

1. Anti-virus and anti-spyware software should be updated on a regular basis.
2. Anti-virus should be set to auto update daily, for example at 12 midnight and then do a scan one half hour later.
3. Anti-spyware should be set to auto update daily, for example at 2:30 AM and then a full system scan one half hour later. This procedure makes sure that only one activity is performed at a time.
4. If the employees work from home, they should also have anti-virus and anti-spyware installed on their home computers.
5. Have anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).**CC**
6. Make sure all anti-virus programs are able to detect, remove, and protect against all known types of malicious software. **CC**
7. Make sure all anti-virus mechanisms are current, actively running, and generate audit logs. **CC**

Install and activate software firewalls on all of your business systems\*

1. Every computer in the network should have its own software firewall enabled.
2. The Microsoft operating system has an built-in firewall, which can be easily located in the Control Panel. Ensure it is always turned on.
3. For other commercial operating system, the operations manual should have instructions about the firewall options.
4. For an added layer of security, commercial firewall software can be installed.
5. Ensure that any employees working with office data at home also adhere to these rules.

Patch your operating systems and applications\*/CC

1. Operating system should be automatically regularly updated with the latest patches and updates provided by the vendors. With Microsoft, this Automatic Update feature is set in the Control Panel, under Security or System.
2. Major software applications like Microsoft Office and Point of Sale software should also be regularly updated with vendor-supplied security patches.
3. Other installed business applications should also be updated on a regular basis.
4. Install critical security patches within one month of release.**CC**

How to dispose of old computers and media\*\*/CC

1. Destroy a hard disk by drilling several holes into it and beating the hard disk platter with a hammer to ensure data is unrecoverable.
2. When media is no longer needed for business or legal reasons, it should be destroyed by shredding, incinerating, or pulping hardcopy materials. Media includes papers containing sensitive information and other removable media (like CD, DVD, USB, floppy drives).
3. When organizations do not follow the proper procedure to destroy sensitive data, identity theft can result, and/or cardholder data may be reconstructed.

Issues in downloading software from the Internet\*\*

1. Software download should be done only from trusted websites like Microsoft for Windows updates and Office application updates.
2. Avoid downloading and using freeware or shareware, since most of them either do not come with technical support or full functionality.

How to get help with information security when you need it\*\*

1. Help or advice should be obtained from a competent, specialized person, when needed.

### Workstation/Laptop Security Configurations

The configurations for workstations and laptops shall include standard software, expected logs, required password complexity, antivirus/firewall security settings, encryption settings, etc. This configuration describes all standard settings.

### Procedures for Change Management

Change Management tracks requests for hardware or software fixes and changes. How do people submit requests for changes? It may be useful to create a Change Management e-mail form, which can be emailed to the system administrator. The form shall contain requestor name, problem or change text, affected machine, priority (1 hour, 1 day, 1 week, 1 month), operating system, date submitted, date fixed, and problem resolution text. The system administrator tracks all Change Management forms.

### Standards or Procedures for Software Installation

Software installation must be controlled, since downloaded software can easily contain viruses and other malware. This section considers how new software is requested, approved, and tested for safety: What standard set of software is installed for various IT users? How can users request specific software to be installed? What is the approval process for new software?

## Network Security

The Standards Section 5.3.1 includes recommendations from NIST that all small businesses should adhere to. Mature organizations shall also retain a copy of their firewall and/or router configurations. The design of these filters is developed during tactical security planning phase: Section 4.2 Planning for Network Security.

### Network Security Standard

The following indicates the priority of the recommendations:

Recommendations with 1 asterisk\*= NISTIR 7621 Absolutely Necessary

Recommendations with 2 asterisk\*\*= NISTIR 7621 Highly Recommended

Recommendation with superscript**CC** = PCI DSS partial implementation

Router/Firewall Configurations\*/CC

The recommended settings to provide security for your organization’s Internet connection:

1. Install a hardware firewall between your office network, the Internet, and your cardholder environment. Change the default password of the router, and if possible, change the default login name.
2. Ensure that any employees working with office data at home also adhere to these rules.
3. Restrict inbound and outbound data into the cardholder environment.**CC**
4. Install perimeter firewalls between any wireless networks and the cardholder environment. Configuration of the firewall should be set to deny or control traffic from the wireless networks into the cardholder data environment.CC
5. Do not allow direct access or any direct connections inbound and outbound between the Internet and the cardholder data environment.CC
6. Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.CC
7. When “established” connections are allowed into the network, ensure stateful inspection. CC

Secure your wireless access point and networks\*

Recommendations to secure wireless access points include:

1. Disable broadcasting of Service Set Identifier (SSID).
2. Change default administrator password.
3. Enable WiFi Protected Access 2 (WPA-2) using the Advanced Encryption Standard (AES) to ensure strong encryption is used while transmitting data.

Do not use vendor–supplied defaults for system passwords and other security parametersCC

1. Before installing a system on the network, vendor- supplied defaults should always be changed, which includes passwords, simple network management protocol (SNMP) community string, and elimination of all unnecessary accounts.
2. Wireless networks connected or transmitting cardholder data should change wireless vendor defaults, including but not only limited to default wireless encryption keys, passwords, and SNMP community strings.
3. Make sure only necessary and secure services, protocols, processes, and necessary items for the function of the system are enabled.

Encrypt transmission of cardholder data within open, public networksCC

1. All administrative access should be encrypted using strong encryption. Use secure technologies such as SSH, VPN, or SSL/TLS for web-based management and other administrative access.
2. Wireless networks are highly prone to attacks. Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices, which should provide strong encryption for authentication and transmission.

Regularly test security systems and processesCC

1. On a quarterly basis, test for the presence of wireless access points and verify authorized wireless access points.
2. An internal vulnerability scan should be performed quarterly.
3. An external vulnerability scan should be performed quarterly with an Approved Scanning Vendor (ASV). ASV’s are approved by the Payment Card Industry Security Standards Council (PCI SSC).
4. After any significant changes in the network, an internal and external vulnerability scan should be performed.

### Router/Firewall Configurations

The configurations for border routers and firewalls shall be defined in this section. This includes IP/Port address permissions, logging configurations, maintenance configurations, and any special security configurations.

## Physical Security

The Standards section includes recommendations from NIST that all small businesses should follow. Mature organizations also keep an inventory of their computer hardware, and audit the hardware regularly (at least annually depending on security needs).

### Physical Security Standard

The following indicates the priority of the recommendations:

Recommendations with 1 asterisk\*= NIST Absolutely Necessary

Recommendations with 2 asterisk\*\*= NIST Highly Recommended

Recommendations with superscript**CC**= PCI DSS partial recommendation

Control physical access to your computers and network components\*

1. Do not allow any unauthorized person to work on your computers.
2. Position your computer’s display to hide information on the screen.
3. Cleaning crew and network repair personnel are often unsupervised in work area. Take precautions.

**Restrict physical access to media containing any cardholder dataCC**

1. Physically secure all affected media.
2. Maintain strict control over the internal and external distribution of affected media.
3. Determine the sensitivity of the data by classifying media.
4. Track sent media by secured courier or other delivery methods.
5. Ensure management approves the transfer of any or all affected media from a secure area, especially when media is distributed to individuals.
6. Maintain strict control over storage and accessibility of affected media.

### Physical Equipment Inventory

Date of Inventory:

Taker of Inventory:

Special Notes: (e.g., software on all computers)

Table 6.4.1: Computer Equipment Inventory

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Location | Owner | Hardware (w. inventory tag #) | Operating System | Licensed  Software  (and license expiration) | Network Address |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Business Continuity

The Standards section includes recommendations from NIST that all small businesses should follow. All organizations shall also define a procedure for backup and restore, particularly for the main server(s).

Mature organizations shall also define procedures for business continuity, incident response, and disaster recovery. These procedures are a logical extension of Sections 3.4 Business Impact Analysis and Business Continuity, and Section 4.5 Planning for Incident Response. For example, for Incident Response, the Tactical security planning Section 4.5 defines the high level procedures. When an incident occurs, Section 4.5 should be consulted and an Incident Response (Appendix A) should be completed. Very mature organizations may define detailed incident response procedures in Section 5.5.4 below.

### Business Continuity Standard

The following indicates the priority of the recommendations:

Recommendations with 1 asterisk\*= NISTIR 7621 Absolutely Necessary

Recommendations with 2 asterisk\*\*= NISTIR 7621 Highly Recommended

Procedures for Back-up and Restore\*

1. Backup should be done (at least) once a week. If possible, store to removable media (e.g., DVD).
2. The removable media should be big enough to hold 52 weeks of backup (e.g., 500GB) and retained separate from the original data, off-line.
3. Do a full backup once a month and store it in off-site location. This would be useful in case of a disaster in your office (fire, theft, flood, etc.). On the removable media create 12 folders for each month.
4. Backup data should be tested periodically to ensure reliability.

### Procedures for Backup and Restore

Data must be backed up on disk or tape. Backup procedures describe how backup is performed. Restore procedures describe how backup data can be reloaded in the event of a disk failure or sabotage.

Questions to be answered include:

Which files are to be backed up?

Who is responsible for performing backups?

Where are backups retained off-site?

How many and for how long are backups retained, and how are they rotated?

What is the naming convention for backup media?

How is the backup and recovery process tested?

How is backup data disposed?

Procedures describing the backup and recovery processes shall be defined.

Recommendations include:

Backups are kept off-site (1 or more)

Off-site library is sufficiently far away (disaster-redundant)

Library is equally secure as main site; unlabelled

Library has constant environmental control (humidity-, temperature-controlled, UPS, smoke/water detectors, fire extinguishers)

Detailed inventory of storage media & files is maintained

### Procedures for Business Continuity

A Business Continuity Plan (BCP) describes how a disaster is declared and how business is resumed on an alternate mode system. The following recommendations are for a large company, and thus should be paired down to apply to your organization’s size.

Recommended steps include:

Employee calls Security Officer

Security Officer declares an emergency.

Security Officer follows predetermined protocol

Human life is first concern

IT follows Disaster Recovery Plan

Phone tree notifies relevant participants

Management and legal counsel act

Public relations interfaces with media (and no one else does)

These recommendations can be scaled down for a small office.

Business continuity procedures must consider:

Evacuation plan: People’s lives take first priority – how do they exit?

Disaster declaration: Who, how, for what?

Responsibility: Who covers necessary disaster recovery functions?

Procedures for Disaster Recovery (next sections)

Procedures for Alternate Mode operation

Resource Allocation: During recovery & continued operation

Testing: Should occur annually via paper-based, partial, or full test.

Copies of the plan should be off-site.

### Procedures for Incident Response

An incident is defined to be any security problem affecting computer systems, networks or data, including, for example, when anti-virus software finds a virus.

High level Incident Response procedures are defined in Tactical security planning Section 4.5 Planning for Incident Response. When an incident occurs, these high level plans shall be consulted, and an Incident Response Form (Appendix A) shall be completed. Detailed Incident Response procedures can be included here, and referenced in Section 4.5.

### Procedures for Disaster Recovery

A Disaster Recovery Plan describes IT procedures for Business Continuity recovery. For example, if the main server system fails, is there an alternate system that should be brought up (as per Section 3.4 Addressing Business Impact Analysis and Business Continuity)?

All BC/DR plans shall be retained online, and via paper-format, on-site, and off-site. IT-specific disaster recovery functions shall consider: software, applications, emergency operations, network recovery, hardware, database/data entry, and information security.

## Personnel Security

The first two subsections of this section list NIST recommendations for a security standard. The first, Physical Security Standard, considers personnel security from an organizational perspective. The second, Computer Use Training and Agreement, considers security rules that all employees shall adhere to when accessing the organizations’ computers. Mature organizations have an Employee Hiring Standard.

A discussion of Separation of Duties, a description of organizational roles and security responsibilities, and required training for these responsibilities are designed in Tactical security planning: Section 4.6 Organizing Personnel Security.

### Personnel Security Standard

The following indicates the priority of the recommendations:

Recommendations with 1 asterisk\*= NISTIR 7621 Absolutely Necessary

Recommendations with 2 asterisk\*\*= NISTIR 7621 Highly Recommended

Recommendation with superscript**CC**= PCI DSS partial implementation

Train your employees in basic security principles\*

1. On the first day of work, employees should be given training on organizational security policies and how to protect sensitive data.
2. Limit use of telephone, printers and other business-owned resources for personal use.
3. Request employees sign a statement that they understand the policies and the penalties for not following them.
4. Security training can also be provided by external sources, such as technical college or commercial training vendors.

Recommended personnel practices in hiring employees\*\*

1. Do a comprehensive background check, including criminal background check, before hiring a new employee, particularly if they will have access to assets or secure information. Other useful checks include credit check and reference check.
2. Verify educational details like GPA, degree, and date of graduation directly from the school.
3. It’s a good idea to do a background check on yourself to learn if you are a victim of identity theft.

Employee Termination

1. When employees are terminated, their authorization and access control privileges shall be revoked.

**Restrict access to cardholder data by business need-to-know**

1. Restrict access rights of users to the least possible privilege necessary to perform their job responsibilities
2. Assignment of privileges should be based on an individual’s job classification and function

### Computer Use Training and Agreement

The following security practices are recommended for employees to be trained for, and to sign as part of their computer use agreement:

How to protect against Social Engineering\*\*

1. Providing sensitive information to strangers pretending to be a part of the organization should be avoided. Any such activity should be reported to the management.
2. Employees should be trained against social engineering attacks from in-person, phone, e-mail, or other electronic methods.

Security concerns about e-mail attachments and e-mails requesting sensitive information\*\*

1. Attachments should be opened only from trusted senders.
2. If you are not expecting an e-mail attachment from the sender, it is a good idea to call and confirm, before opening the attachment.
3. Spam e-mail often asks for sensitive information.

Security concerns about web links in email, instant messages, social media, or other means\*\*

1. Never click on a link in an e-mail attachment, except only when you are expecting it.
2. If you are not expecting an e-mail link from the sender, it’s a good idea to call and confirm, before clicking on the e-mail link.
3. If you hover the cursor over an e-mail’s Web link description, the link should be displayed on the bottom of the browser. Make sure both of them match and the Web link looks valid.

Security concerns about popup windows and other hacker tricks\*\*

1. Do not respond to pop ups while working online. For example, a malicious pop up message may say that you have a virus on the system. Close it by clicking on X in the upper right corner. If you click OK, it might install spyware or other malicious code.
2. Infected USB drives are often left unattended by hackers in public places. They intend for unsuspecting people to take the USB home or to the office and unknowingly install the worm or malicious code. For additional protection, disable the “AutoRun” feature for USB drives.

Doing online business or banking more securely\*\*

1. Always used secure browser to do online activities. Before entering secure data, ensure a small lock appears in the bottom right of the screen.
2. Frequently delete temp files, cookies, history, saved passwords etc. On Windows Internet Explorer this is accomplished via Tools->Options->General->Delete. On Mozilla Firefox use Tools->Clear Private Data, and Tools->Options->Privacy->Show Cookies->Remove All Cookies.

Security considerations for web surfing\*\*

1. Never use an admin account to surf the Web. If there was a compromise the malicious code would have admin rights.

Standard Security Precautions (last, but possibly most important)

1. Promise to not divulge login IDs and passwords

1. Create quality passwords according to company standard
2. Lock terminal when not present
3. Report suspected violations of security
4. Maintain good physical security (locked doors, private keys)
5. Conform to laws and regulations
6. Use IT resources only for authorized business purposes

### Employee Hiring Standard

New employees should be hired according to a standard. It is more important to have a standard than to have a perfect standard. The standard should be realistic with actual expectations of what is most important. It is perfectly permissible to delete sections that you think will be too much work. In fact, if employees think an organization is too restrictive without understanding why, they will not want to work for the organization. Thus, if the rule does not represent the needs of the organization or is too strict, it may be good to forego the rule.

New employee signs document that he or she has read and will adhere to security policies. New employee training includes dealing with Social Engineering, computer attacks, and security, including information protection.

# References

Appendix A: Incident Response Report

|  |  |  |
| --- | --- | --- |
| **Discovery** | | |
| Date: | | Reviewed By: |
|
| Incident: | | |
|
| Individuals Involved: | | |
|
| From where did the attack originate? | | When was the attack first discovered? |
|
| How was the attack discovered? | | |
|
| How did the incident occur? | | |
|
|
| Reason or vulnerability that allowed or caused incident: | | |
|
|
| What is the reason for the vulnerability? | | |
|
| **Recovery** | | |
| Was the problem resolved? | | Who completed the recovery? |
| If so, when? | |
| What functions did he or she perform? | | |
|
|
| What tests were performed to ensure functionality? | | |
|
|
| **Improvement** | | |
| What went right or wrong in the incident response? | | |
|
|
| How can process improvement occur? | | |
|
|
| **Incident Cost** | | |
| Actual Loss: | $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Time allocated: |
| Response Cost: | $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| TOTAL LOSS: | $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Appendix B: IT Governance & Planning

B.1 Strategic Planning

Strategic planning is the highest level of IT Governance planning involving directors and executives. Long-term (3-5 year) direction considers organizational goals, regulation (and for IT: technical advances). In Table B1, the objectives can be listed and a timeframe of completion or compliance can be given.

Table B1: Strategic Plans

|  |  |
| --- | --- |
| **Objective** | **Timeframe** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

B.2 Tactical Planning – Year 1

Tactical planning is concerned with objectives that are expected to be completed within one year. The one year plan moves organization to strategic goal. In Table B2, the objectives can be listed and a timeframe of completion or compliance can be given.

Table B2: Tactical Plans

|  |  |
| --- | --- |
| **Objective** | **Timeframe** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Operational Planning – Quarter 1 of Year 1

Operational planning is concerned with short term technical plans. These plans are more detailed and are tasked to individuals for completion or compliance. Basically, this level of planning lists how the objectives in the Tactical Plan will be completed, who will do what and how long it should take. In Table B3, the objectives and a timeframe can be listed and the responsible individual(s) can be named.

Table B3: Operational Plans

|  |  |  |  |
| --- | --- | --- | --- |
| **Objective** | **Responsibility** | **Deliverable** | **Timeline** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. [↑](#endnote-ref-2)
2. Richard Kissel, NISTIR 7621, “Small Business Information Security: The Fundamentals (Draft)”, National Institute of Standards and Technology, U.S. Dept. of Commerce, May 2009, <http://csrc.nist.gov/publications/drafts/ir-7621/draft-nistir-7621.pdf>. [↑](#endnote-ref-3)
3. COBIT 4.1, IT Governance Institute, www.itgi.org. [↑](#endnote-ref-4)
4. CISA Review Manual 2009. (Certified Information Systems Auditor) ISACA, www.isaca.org. [↑](#endnote-ref-5)
5. CISM Review Manual 2009. (Certified Information Security Manager) ISACA, www.isaca.org. [↑](#endnote-ref-6)
6. This Code of Ethics is adapted from “Essentials of Corporate Fraud”, Tracy L Coenen, John Wiley & Sons, 2008. [↑](#footnote-ref-2)