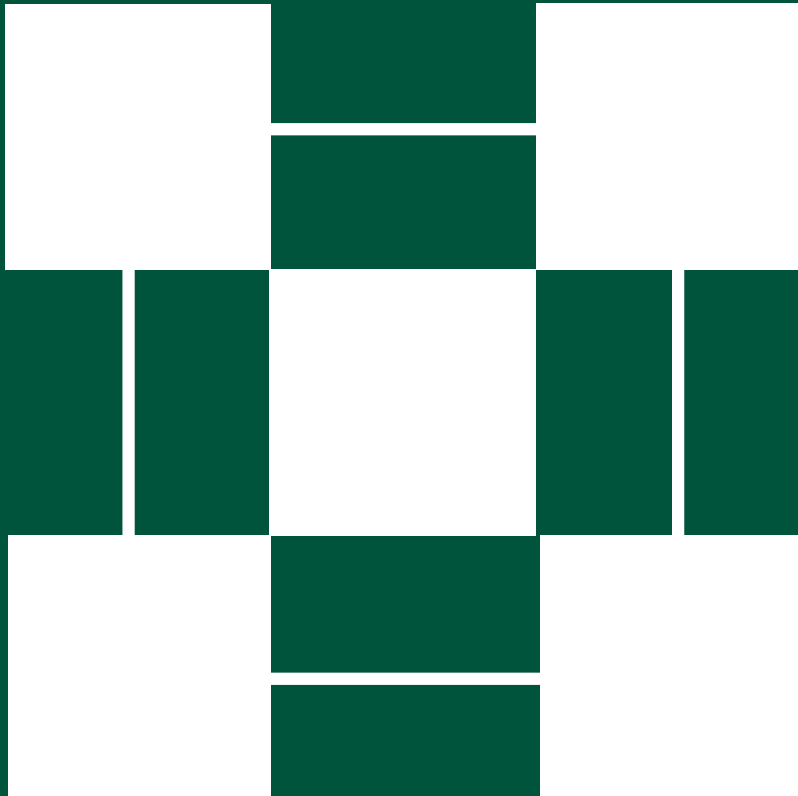


# Basic Security Program Components



**MBA Residential Technology  
Steering Committee (ResTech)**

Information Security Subgroup

May 2008



Contents

<b>I. Introduction</b>	<b>1</b>
<b>II. Acceptable Use Policy</b>	<b>3</b>
A. Acceptable Use of Employee Workstations	3
B. Acceptable Use of Internet and Email	4
C. Acceptable Use of Data	5
D. Acceptable Use of Software	5
<b>III. User Access Control</b>	<b>7</b>
A. Fundamental Access Controls	7
B. Common Risks	7
C. Mitigation Approaches	8
<b>IV. Physical and Environmental Security</b>	<b>10</b>
A. Facility and External Environment	10
B. Inside the Facility	10
<b>V. Personnel Security</b>	<b>12</b>
A. Common Risks	12
B. Mitigation Approaches	12
<b>VI. Business Continuity Planning</b>	<b>14</b>
A. Common Risks	14
B. Mitigation Approaches	14
<b>VII. Compliance</b>	<b>15</b>
A. Common Risks	15
B. Mitigation Approaches	16
<b>VIII. Third-Party Provider Management</b>	<b>17</b>
A. Common Risks	17
B. Mitigation Approaches	17
<b>IX. Technology Security</b>	<b>18</b>
A. Common Risks	18
B. Mitigation Approaches	18
<b>X. Future Actions</b>	<b>20</b>
<b>XI. Glossary</b>	<b>21</b>
<b>XII. References</b>	<b>23</b>

# I. Introduction

As public concern escalates for the protection of personal information and the compliance with statutes and regulations, the demand on an organization's Information Security Program (Info Sec Program) also intensifies. The number of threats, and the complexity of addressing them, is increasing as well. Hacked systems, spyware, lost personal information and insider theft are some examples of the threats that organizations must mitigate. While information security does not generate revenue, the costs associated with liability, reputation and compliance failures obligate senior managers to pay attention.

Regardless of their size, most companies are expanding the scope of information asset protection and spending more for it. This heightened attention started with the Enron accounting debacle, which resulted in the enactment of the Sarbanes-Oxley Act (SOX)<sup>1</sup> on July 30, 2002. SOX dramatically changed the regulation of financial practice and corporate governance. California Senate Bill 1386 (CA SB 1386), introduced in July 2003, was the first attempt to address the problem of identity theft ever made by a state. The bill requires companies and government agencies suffering from unauthorized access to the personal information that they store to notify California residents who are potentially affected. The February 2005 Choice Point security breach, during which thieves opened fifty accounts to access Choice Point's databases of personal information, provides still more evidence of the need for improved controls. Regulators across all jurisdictions have issued guidance about protecting information and made multiple audit requirements for it. The unfortunate trend is for more regulation, not less.

Large corporations have the necessary fiscal and human resources to comply with the growing number of regulatory requirements. Small and mid-sized organizations face similar requirements, but have far fewer resources. The extent to which these smaller organizations manage their resources efficiently and effectively is the difference between the assurance that risks have been reasonably mitigated and the constant fear of impending breach. There is no silver bullet. All companies need to identify, manage and mitigate risks to their information assets.

This paper identifies eight major components of an Info Sec Program:

1. Acceptable Use Policy
2. User Access Controls
3. Physical Security
4. Personnel Security
5. Business Continuity Planning
6. Compliance
7. Third-party Provider Management
8. Technology Security

---

<sup>1</sup> Public Law 107-204. Also known as the "Public Company Accounting Reform and Investor Protection Act of 2002."

## Identify, Manage, and Mitigate Risks to Information Assets

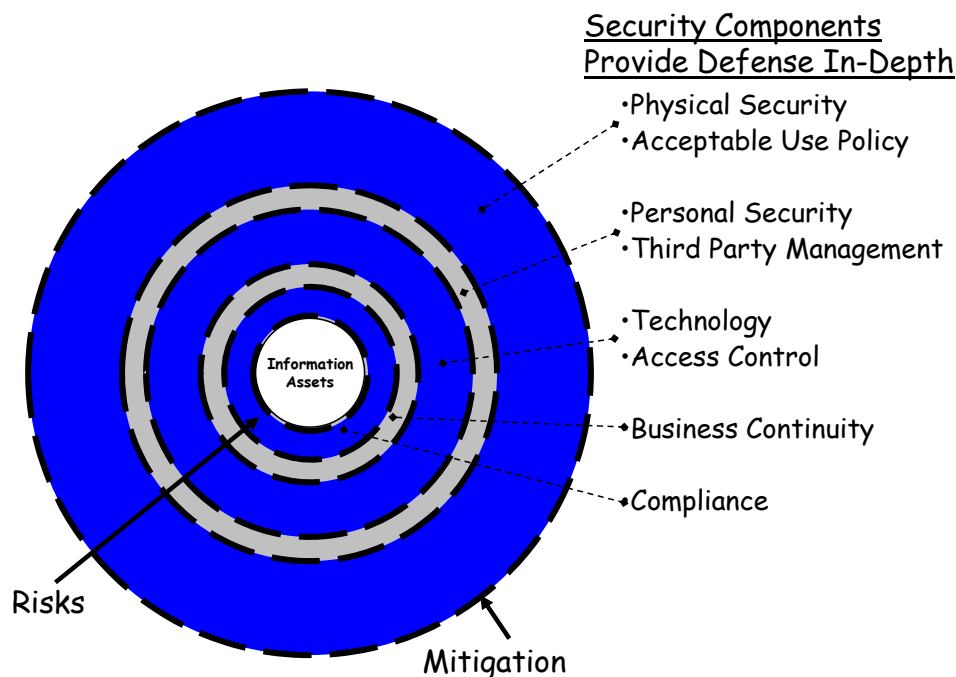


Figure 1 - Information Security Program Diagram

The unfortunate fact is that the protection of assets is an unremitting activity. Once a program is established, it will need to be measured, tested and modified over time. Lines of business, roles, technologies, threats and vulnerabilities change. Employee and customer awareness programs must reflect the changing environment.

While the security standards of organizations might differ on the number and names of their components, there are common areas of interest addressed by most of them. The intent of this paper is not to reproduce well-known standards, but rather to identify the minimum set of objectives that small and mid-sized organizations must meet in order to execute an effective Info Sec Program. This concise and business-oriented approach will help guide small and mid-sized organizations with limited resources.

Guidance, however, does not guarantee compliance with state or Federal regulations or with business partner requirements. Nor is it a substitute for legal advice. Readers should consult a qualified legal counsel regarding the compliance and legal requirements of their organizations.

Information security is a rapidly developing field. As the environment develops and matures, organizations should monitor related laws, technologies and industry practices to ensure the ongoing effectiveness and relevance of their Info Sec Programs.

## II. Acceptable Use Policy

All effective security starts with educated and informed users. Your organization can avoid some basic risks by establishing general rules for the use of technology, documented in what is known as an “Acceptable Use Policy” (AUP). AUPs should address the following topics, many of which are not technical in nature, but rather focus on productivity and human resource issues.

### A. *Acceptable Use of Employee Workstations*

Employee workstations consist of any automated or manual tools employees need to do their jobs: desktop or laptop computers; network connections, printers, scanners or fax machines; portable media like thumb drives and CDs; and paper files or corporate manuals.

#### 1. *Common Risks*

- a. **Unauthorized access to systems and data.** Employees might install freeware on their computers that has not been checked against your organization’s AUP, accidentally installing spyware or crimeware that exposes corporate information to unauthorized individuals.
- b. **System failure due to improper environmental controls.** Desktop computers are especially sensitive to environmental factors such as smoke, dust, heat, humidity, food particles and liquids. Because of their portability, laptop computers can be exposed to additional environmental factors, such as extreme temperatures and moisture, when they are taken from the office or left in a car.
- c. **System incompatibility.** Employees might install software on their computers that is not authorized by your organization’s AUP. If the unauthorized software is not compatible with your business software, it could cause unintended system malfunctions or reduced productivity.
- d. **System outage.** The occurrence of any combination of the risks described above can lead to the complete outage of the affected employee’s system.

#### 2. *Mitigation Approaches*

In order to address the common risks described above, your organization should document how employees are expected to use their workstations. Employees need to know what care and maintenance tasks they are required to perform as well as what types of software they may load or use.

- a. **Log Off and Power Off Daily.** Requiring employees to log out of any networks or applications and to shut off their computers before leaving for the day will prevent the use of unauthorized workstations. This practice also provides the power downtime some software patches need to be fully installed.
- b. **Secure the Workstation during Business Hours.** Expecting employees to lock their workstations before leaving them or to use software-locking features after specified periods of inactivity will prevent systems and applications from being used at unauthorized access levels during their absence.
- c. **Comply with Environmental Controls.** Your organization’s AUP should provide guidance about the proper care of workstations, including the steps employees must take to keep work areas clean and safe from environmental risks. The AUP should

clearly document the safeguards employees must practice when they remove a laptop from their work locations, along with any liability employees bear if the laptop is lost or damaged while off-site.

- d. **Practice Password Safety.** The AUP documents your organization's policy about storing workstation passwords. In many cases, a documented password is acceptable if the employee stores the document securely.
- e. **Require Protective Software.** Your organization's AUP should list the protective software that must be installed on each workstation, including anti-virus software, local firewalls, client patches and asset management applications.

## **B. Acceptable Use of Internet and Email**

### **1. Common Risks**

In most organizations, employees regularly use email and access the internet while performing their assigned duties. Some of the risks described below are present even during authorized internet use. For example, one of your employees could access an illegal, pornographic, harassing or malicious website completely by accident. However, these occurrences should be the exception within your organization.

- a. **Productivity Loss.** Employees might use the internet and either corporate or private email for personal purposes during work hours, reducing the amount of time they spend on assigned duties. Additionally, employees accessing streaming media can negatively affect the availability of your organization's network resources.
- b. **Personnel Issues.** Employees using the corporate internet can access illegal or pornographic websites. They might also access websites that subsequently send volumes of harassing email.
- c. **Infections.** Malicious websites could infect an accessing workstation with a virus, Trojan horse or spyware without the knowledge of the employee visiting the site.
- d. **Disclosure of Customer or Proprietary information.** Employees can use personal email or Instant Messengers from their workstations to send information out of the company, bypassing any information security controls you might have in place.
- e. **Spamming.** If your organization sends out large volumes of direct email as part of its normal business practices, it risks being blacklisted as a spammer.

### **2. Mitigation Approaches**

- a. **Document Definitions and Consequences.** Your organization's AUP should clearly define the difference between acceptable and non-acceptable use of corporate email and the internet during both work and non-work hours. The policy should spell out consequences of deliberate employee access of illegal or pornographic websites.
- b. **Use Internet Filters or Proxies.** Consider using an internet filter or proxy to monitor and manage internet access.
- c. **Be Careful with Mass Mailings.** The AUP should address mass mailings to customers and potential customers. Most Internet Service Providers have rules regarding the use of their systems for sending mass email communications.

## C. Acceptable Use of Data

### 1. Common Risks

- a. **Financial Privacy Rule Compliance Failures.** The Gramm-Leach-Bliley Act's<sup>2</sup> (*GLBA's*) *Financial Privacy Rule* governs the collection and disclosure of customers' personal financial information by financial institutions and by any company receiving such information. *The Safeguards Rule* requires all financial institutions—whether collecting information from customers or other financial institutions—to design, implement and maintain safeguards to protect customer information. GLBA compliance is mandatory. Whether or not a financial institution discloses nonpublic information, it must have a policy in place to protect the information from foreseeable threats to security and data integrity.
- b. **Data Breaches.** If your company is identified as the source of a data breach, the damage to your corporate reputation and the costs of litigation can be extremely serious. Data breaches occur when company laptops, removable USB drives or CDs containing private information are lost or stolen, when malicious employees sell corporate data and when unsecured systems are accessed from outside the corporate firewall.

### 2. Mitigation Approaches

You can reduce the risk of data breaches that are the result of lost or stolen workstation assets by including the organization's policy for securing workstations in the AUP.

- a. **Document Policy.** At a minimum, your organization's AUP should describe the proper use of corporate data: what is and is not allowed.
- b. **Explore Technical Controls.** Consider implementing specific technical controls based on your size, the nature of the data you process and the results of a risk assessment.

## D. Acceptable Use of Software

### 1. Common Risks

- a. Malicious Software Bundled with Freeware
- b. Unlicensed Software (or software with an expired license)
- c. Purchased Software that is Incompatible with Approved Software
- d. Out-of-date Software Patches and Support

### 2. Mitigation Approaches

- a. **Install Only Purchased Software.** Allow only purchased software to be installed on any machine that connects to your network or is used for company business.
- b. **Installation Only Approved Software.** Allowing only approved software to be installed on your organization's computer equipment is a reasonable and prudent

---

<sup>2</sup> Public Law 106-102. Also known as the Gramm-Leach-Bliley Financial Services Modernization Act.

policy, but enforcing it can be a challenge. Companies determining the need for such a policy must also create an enforcement plan and then secure the required resources to implement it.

- c. Test All Software Prior to Installation.** Test any software that is to be installed for corporate use to ensure that it is compatible with other business-critical software and applications. Compatibility issues regularly arise with JAVA versions, software patches for operating systems and browsers, and anti-virus software.
- c. Document a Software Support and Maintenance Plan.** All organizations should document a software support plan and a method for deploying patches. The plan should include both official business software and unsupported software. For example, even if your organization does not support the use of MP3 players by employees at their workstations, it is a prudent policy to install all available security patches. An MP3 player is just as vulnerable to exploitation while attached to the employee's workstation as the workstation's own operating system.

## III. User Access Controls

Properly implemented and managed, automated systems enable small and mid-sized mortgage companies to compete effectively with the mortgage giants. However, if user access to these systems is not properly controlled, critical information can be compromised or destroyed. No matter how small the organization, someone must be accountable for ensuring that proper user access controls are in place.

### A. Fundamental User Access Controls

The three fundamental user access controls are:

1. **Initial Identification.** The process related to the first identification of an individual (or device).
2. **Identity Credential Administration.** The life-cycle management of the identity credential (for example, password or digital certificate). Credentials are referred to generically as factors, and are defined in terms of the point of view of the user trying to gain access:
  - a. **Something You Know.** Memory triggers such as passwords, PINs, questions or images.
  - b. **Something You Have.** Physical objects such as digital certificates, tokens or Smartcards.
  - c. **Something You Are.** Biometric data such as fingerprints or signatures.

Factors are used to mitigate risk when authorizing access to applications or information. The strength of a physical object (Something You Have), or the confidence in it, is generally stronger than a password or PIN (Something You Know). Biometric data is generally considered the strongest of the three factors. Factors can be combined and used together to improve the strength of access controls, a process known as multi-factor security.

3. **Authorization.** Validation and assignment of credentials to individuals.

### B. Common Risks

1. Unauthorized access to information, systems and networks
2. Unauthorized modification or disposal of information
3. Unauthorized access to information, systems and networks through mobile or tele-networking facilities
4. Undetected access to information, systems and networks
5. Undetected modification or disposal of information
6. Insufficient access controls for the risk classification (low, medium or high) of the information
7. Unsatisfactory internal or external audit reports due to failure to establish adequate access controls

8. Exposure to lawsuits and regulatory fines and sanctions if a data breach results from unauthorized access

### **C. Mitigation Approaches**

1. **Select Acceptable Proofs of Identification** for employees and business partners. Proofs include but are not limited to Federally- or State-issued identification cards, passports, Social Security Number (SSN) or business references from a source such as Dun and Bradstreet.
2. **Establish Policies for Credential Lifecycle Management.** Credential policies include but are not limited to password length, data type, history and storage of private keys.
3. **Classify Risks to Systems and Information** as low, medium or high so that you can protect them with appropriate user authorization and access codes. Financial regulators require strong authentication for high-risk transactions, which typically include financial transactions or exchanges of personal identifiable information. The use of a password is insufficient as a single factor access control for high-risk transactions.
4. **Establish User Authorization Criteria and Access Controls** to sensitive information. Managers of accessible information resources provide the actual access controls to authorized employees.
5. **Identify Administrator Roles** and provide strong access control for administrator activities.
6. **Manage Authorized Employees.** Managers must make sure the system users for whom they are responsible:
  - a. Have the access controls and resources needed to perform their jobs;
  - b. Lose access when they are terminated or when job responsibilities change;
  - c. Sign confidentiality statements if required.
7. **Establish an Audit Log** of any access to sensitive information. At a minimum, the log should include system identification, user name and the date and time of access. Routinely monitor the log to detect violations and weaknesses.
8. **Train Employees** to use access controls effectively. Require employees to acknowledge that they understand the requirements and agree to comply with them.
9. **Manage Remote Access.** Remote access connections to corporate networks should meet the same levels of control as on-site connections.
  - a. Develop an Acceptable Use Policy for remote access that governs access through Virtual Private Networks (VPN), terminal servers and remote wireless devices. The business-to-business frame relay must meet the minimum authentication requirements of Data Link Control Identifier (DLCI) standards.<sup>3</sup>

---

<sup>3</sup> For more information on DLCI visit:  
[www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan\\_c/wcfapdx/wcfappa.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfapdx/wcfappa.htm).

- b. Strictly enforce remote access controls with password authentication or public/private keys with strong passphrases.
- c. Limit simultaneous access to non-corporate networks. Users with remote access privileges must ensure that their corporate-owned or personal computer, when remotely connected to the corporate network, is not connected to any other network at the same time. Personal networks that are under the complete control of the user are acceptable exceptions.
- d. Require your Information Technology (IT) department to approve all non-standard hardware configurations and remote access connections to your corporate production network.
- e. Require all computers that have remote access to your corporate networks to use up-to-date antivirus, anti-spyware and personal firewall software such as Windows XP Pro SP2 Firewall, Zone Alarm or Norton. Third party connections must comply with your organization's AUP.

## IV. Physical and Environmental Security

Brick-and-mortar is a well-established environment. Whether the objective is to secure home or office, the basic concepts of safeguarding property and possessions are similar. These controls are extended to secure business equipment, personnel and assets. In order to do this effectively, it is critical that organizations identify and classify as low, medium or high the risks to business facilities, equipment, files, other assets and personnel. The risk classifications will help determine the appropriate type of security controls to implement in each case.

### A. Facility and External Environment

#### 1. Common Risks

- a. Unauthorized physical access to the facility and surrounding perimeter
- b. Damage to business property or interference with it
- c. Interruption of business activities

#### 2. Mitigation Approaches

- a. **Protect against External and Environmental Threats.** The external environment—weather and natural or man-made disasters—can have a severe impact on business operations. Mitigation measures for these risks are usually documented in an organization's Business Continuity Plan (BCP)<sup>4</sup>. The BCP identifies and assigns responsibilities to employees for the management of a variety of environmental events.
- b. **Establish Physical Security Perimeter.** Be aware of the facility's perimeter and vulnerabilities as well as the potential threats to it. Identify security controls that can reduce exposure to these risks—for example, cameras, parking lot lighting or agreements with neighbors.
- c. **Establish Physical Entry Controls.** Develop basic policies and procedures for gaining physical access to the facility (including loading areas). These should include rules governing employee, delivery service and public access. Monitor all access and keep an entry log to provide important historical and audit information.

### B. Inside the Facility

#### 1. Common Risks

- a. Unauthorized physical access to interior infrastructure, offices, rooms or storage areas
- b. Damage to business property; interference with it
- c. Damage, loss or compromise of assets
- d. Damage, modification or theft of information assets; interference with them

---

<sup>4</sup> See Section VI.

## 2. Mitigation Approaches

- a. **Protect Supporting Infrastructure and Equipment.** Power equipment, power cabling, network cabling, servers, printers and fax machines are the enabling technologies that support your business operations. Infrastructure maintenance is an activity that organizations often overlook. Create policies governing the maintenance, replacement, upgrade and periodic testing of infrastructure items, including the cables and the smoke and fire alarms. More importantly, the policies should have provisions to confirm that these activities are scheduled and completed in a way that ensures continuous business operations.
- b. **Identify and Secure Offices, Rooms and Storage Areas.** Those which contain confidential information should have stronger security mechanisms, including an entry log to provide important historical and audit information.
- c. **Practice Proper Equipment Maintenance.** Maintenance of business equipment and software is critical. Regularly applied software updates and patches can prevent many of today's virus attacks. Purchase and use spyware and anti-virus products, enable automatic updates and monitor security news links for threats and vulnerabilities. Logging any policy lapses or security breaches and then monitoring the log can provide valuable insight into the status of your business operations.
- d. **Establish Security Policy Specifically Addressing Off-Site Equipment.** One of today's greatest threats is posed by the increasing use of off-site equipment and portable media. Laptops, flash drives, CDs, DVDs, backup tapes and *paper* all expose companies to risks. Organizations need to inventory off-site equipment and media, documenting the business activity or activities supported by it. The next step is to develop guidelines and policies governing the removal of equipment containing confidential information from the business facility. For example, backup tapes, including private information and information stored off-site, should be encrypted. Laptop computers might need stronger authentication mechanisms and data files that have additional encryption. Personnel regularly using laptops that contain private information need training on the risks associated with unauthorized disclosure.
- e. **Practice Secure Disposal and Re-use of Equipment.** No company wants to be the subject of a newspaper article describing the private information that was found in the dumpster outside its office. It is just as critical to safeguard data that might be stored on equipment that is to be removed as it is to safeguard it while the equipment is still inside the facility. Organizations should create policies and procedures governing the disposal or removal of any piece of business equipment or electronic media that could contain confidential information. Such a policy includes the requirement to clear servers, computers, tapes, CDs, DVDs and flash drives of confidential information prior to disposal.

## V. Personnel Security

Personnel security is one of the hottest topics in the field today. An important personnel security concept is “the principle of least use,” which promotes the restriction of access rights to sensitive information only to the individuals who need the information to do their jobs. For example, a teller at the branch office may not require access to a customer’s full SSN. The same is true of many other individuals involved in the loan process. Concerns about the liability, and the risk to public reputation, associated with requirements to disclose unauthorized access to personal information have caused many businesses to reevaluate their employees’ rights to information.

### A. Common Risks

1. Harm from intentional or unintentional human actions, including theft, fraud or misuse of resources
2. Harm from security incidents which result in unauthorized access to personal identifiable information
3. Vulnerabilities to data exposures by your customers and business partners
4. Business processes and services that do not comply with the organization's Personnel Security Policy

### B. Mitigation Approaches

1. **Establish Personnel Security Policies and Procedures.** Establish and communicate to all personnel high-level digital rights and management policies governing manual and automated processes and technology. Require employees and business partners to protect personal information; for example, by implementing a clean desk policy.
2. **Conduct Background Checks and Screening.** It is important for your company to know its potential employees, current employees and third-party personnel. The role and responsibilities of a candidate, employee or consultant dictate the proper level of due diligence—background checks and other screening procedures—to be performed during the hiring and contracting processes.
3. **Require Agreements: Confidentiality, Non-Disclosure and Authorized Use.** Clearly define the obligations of both your company and your employees.
4. **Document Job Descriptions: Roles and Responsibilities.** Clearly define the roles of your employees and business partners, and identify what information they have the right to access. Understand data sensitivity classifications (for example, low, medium or high) and apply appropriate authentication controls. For highly sensitive data, you might wish to require “Something You Have” or multi-factor authentication.
5. **Separate and Rotate Duties.** Separation of duties and cross training can be beneficial tools for a small to mid-sized business. The requirement to have more than one individual scan log, or to rotate that responsibility periodically, can reduce vulnerability to a rogue employee.
6. **Provide Awareness Training.** A “low-hanging fruit” that consistently returns maximum benefits is the provision of employee security training—both formally and by example. Senior management must express and demonstrate the importance of the corporate

security policies and encourage employees to notify them of any threats to business information. Employees must be instructed on what is involved in the Clean Desk Policy, like locking up loan files whenever leaving the desk, and in the Off-site Equipment and Media Security Policy, like protecting private customer data on portable media.

7. **Remove Access Rights upon Employee Termination.** Document a set of security procedures to be followed when an employee is terminated. Activities should include cancelling User IDs; confiscating physical access PINS or Fobs; and receiving business equipment, portable media and paper documents. It is useful to create a checklist of the specific out-processing tasks and activities to be conducted by each department.
8. **Document and Impose Sanctions.** Document and enforce the repercussions of noncompliance, with any of your organization's security policies, through administrative penalties.

## VI. Business Continuity Planning

The welfare of employees and the quick resumption of normal business activities are the primary objectives of business continuity. Business Continuity—or Contingency—Planning (BCP) is the ongoing process of identifying the risks of potential interruptions to business operations. Interruptions can result from large-scale natural or man-made disasters as well as from the less destructive events that affect personnel or services. BCP enables a company to minimize financial losses, avoid costly penalties and meet legal and contractual obligations to customers and shareholders.

The purpose of BCP is to mitigate the effects of disruptions. It pre-defines the actions that personnel will take following a disruptive incident, what functions and resources are necessary to recover critical business operations, and what documented steps need to be followed. Critical business functions are those which affect revenue, have legal ramifications, are mandated by regulatory agencies, or which severely impact customer service or public credibility. The ability to resume operation of these functions within the first two weeks of a business interruption is essential to your organization's long-term recovery.

### A. Common Risks

The goal of BCP is to minimize the risk and impact of business interruptions on operations, providing an acceptable level of business functionality until normal operations can be resumed. Risks can be categorized according to the scope of their impact.

1. **Departmental Risk** affects a single department
2. **Building or Facility Risk** affects the facility wherein department is located
3. **Local Impact** affects the business district wherein department is located
4. **Regional Impact** affects an entire city or region wherein department is located

### B. Mitigation Approaches

1. **Create Business Function Continuity Plan.** Document the processes to be followed during an incident.
  - a. Identify critical business functions based on a Business Impact Assessment
  - b. Identify business resources required to support critical business functions
  - c. List the supplies needed to support critical business functions
  - d. Document procedures for safeguarding vital records and equipment
  - e. Identify all disaster recovery locations
2. **Document Communication Plan**
  - a. Identify customers to be notified
  - b. Identify vendors to be notified
  - c. Establish an Employee Notification Tree and notification method(s)
  - d. Identify a Recovery Team
  - e. Draft a Disaster Declaration

## VII. Compliance

Over the last several years, demand has increased for improved security mechanisms. Most organizations have felt the impact of security requirements for internal, regulatory and business partner information. The risks to your organization of noncompliance are criminal, civil, statutory, regulatory or contractual penalties. The development and execution of organizational security policies and standards will maximize compliance and minimize the resources your organization has to spend to undergo internal and external compliance audits.

### A. Common Risks

The risks described in this section are noncompliance with the following statutes and regulations:

1. **Gramm-Leach-Bliley Act (Section 501).** All financial institutions are to establish policies to protect the security and confidentiality of their customer's nonpublic personal information. Furthermore, the establishment of standards for the administrative, technical and physical safeguards to protect against anticipated threats and unauthorized access that can present potential harm to any customer's confidentiality, integrity or availability to nonpublic personal information.
  - a. Safeguarding customer personal information
  - b. Protecting against threats, hazards and unauthorized access
2. **PATRIOT Act<sup>5</sup> (Section 326).** The U.S. Patriot Act was signed into law in response to the attacks against the United States on September 11, 2001. A portion of that legislation defines the requirements for businesses to better understand who their customers are before engaging in financial transactions with them. The regulations require written Customer Identification Programs (CIPs) appropriate to the institution.
  - a. Verifying identity, maintaining records and consulting the government list of known terrorists
  - b. Customer Identification Programs (CIPs)
  - c. Authentication policies and procedures
3. **Information Security Breach Notification Legislation.** More than thirty-five states have enacted legislation similar to California Senate Bill 1386 (CA SB 1386), introduced in July 2003, requiring organizations to notify stakeholders of unauthorized access to private information.
4. **Federal Financial Institutions Examination Council (FFIEC) Guidelines.**
  - a. Customer Identification Programs
  - b. Authentication in Internet Banking
  - c. Response Program for Unauthorized Access

---

<sup>5</sup> Public Law 107-56. Acronym stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." Enacted October 26, 2001. Renewed March 9, 2006.

**5. Federal Trade Commission (FTC) Regulations.**

a. Personal Information Safeguarding Rules

**6. Red Flag Identity Theft.** The Red Flag ID Theft regulation is an amendment to the Fair and Accurate Credit Transactions (“FACT”) Act. Congress, concerned about several emerging issues, including the increasing incidence of identity theft, has made new obligations for lenders and others to prevent, detect and mitigate ID theft. This regulation requires entities to develop written ID theft prevention programs.

**B. Mitigation Approaches**

- 1. Identify Applicable Legislation and Regulations.** For example, GLBA, PATRIOT Act, FTC Safeguard Rules and the Red Flag Identity Theft regulation.
- 2. Identify Contractual Requirements.** For the protection of Intellectual Property Rights (IPR), software licenses, business partner obligations and other legal requirements.
- 3. Protect Organizational Records.** This is a critical requirement. Sarbanes-Oxley (SOX) prescribes safeguards for financial information records. The mortgage banking industry is required to protect the artifacts used to generate promissory notes.
- 4. Protect Personal Information.** Organizational use of personal information is a growing concern of the public and private sectors. Identify sensitive information, the systems using that information, and the network paths along which it travels. Apply security controls to appropriate information, systems and network components in proportion to their risk potential.
- 5. Document and Enforce Information Audit Requirements.** Whether or not your organization is audited regularly, it should write specific audit requirements and then automate their implementation wherever possible. Establish logs to record access to sensitive information, monitor the logs and verify compliance with security policies and audit requirements.
- 6. Regularly Review Legislation, Regulations, Contractual Obligations and Security Controls.** Laws, people and technology change constantly. Monitoring potential changes to your security requirements will help your organization prepare for new compliance obligations. Subscribing to monitoring services like *AllRegs* can make this task manageable.
- 7. Leverage Certification, Accreditation and Security Assessments.** To comply with certain requirements.

## VIII. Third-Party Provider Management

As the saying goes, “You are only as strong as your weakest link.” In the case of information security, third-party providers and vendors can be that “weakest link” if adequate measures are not in place to assess the risk they pose to your organization. Often third-party vendors house some of a company’s most sensitive information, for example, outsourced HR and payroll systems, off-site backups and paper files, and consultants’ unencrypted laptops. Therefore, their procedures for safeguarding that information should be evaluated against your own Information Security Policies (ISP).

### A. Common Risks

The risks described in this section are associated with weaknesses in the third-party provider’s information security policies and procedures.

1. Inadequate security policies and procedures at provider location
2. Unacceptable application vulnerability assessments
3. Inability to manage, monitor and measure service and licensed software providers
4. Retention and storage of unnecessary confidential information
5. No Incident Response Procedures (IRP) or notification mechanism
6. No Business Continuity Plan (BCP)

### B. Mitigation Approaches

1. **Verify and Document All Current Third-Party Vendors** serving your organization. Include outsourcing arrangements, employment agencies, software vendors, janitorial maintenance and outside legal counsel.
2. **Assess and Rank Vendors Based on the Level of Risk** they pose—for example the sensitivity or volume of information they store or process, or the criticality of the business functions they provide.
3. **Conduct More Substantial Investigation of Highest Risk Vendors** and their security controls.
4. **Use Open Standards and Best Practices as Criteria for Establishing Relationships.** SAS 70 (Type 2), AICPA Trust Services, National Institute of Technology and Standards (NIST) and other well-known certifications and/or accreditations can provide independent third-party assurances of the security services or solutions.
5. **Require Licensed Software Providers to Adhere to a Set of Software Development Methodologies.** Require vendors to document their approaches to preventing malicious code, reducing vulnerabilities and conducting maintenance.
6. **Require Remediation or Acceptable Mitigating Controls** for identified vulnerabilities.
7. **Continue to Monitor Annually.** At minimum.

## IX. Technology Security

Participants in the mortgage banking industry should manage technology assets—network, system, and application hardware and software—from acquisition to disposal in accordance with the best practices of asset protection control. In today’s environment, the technological components of these controls are critical, and organizations must leverage them, along with people and processes, to provide effective technology security.

### A. Common Risks

1. **Data Leakages.** Compromises to information confidentiality.
  - a. Compromise of assets from a third party, business partner, eBusiness transaction, internet access, hackers or viruses
  - b. Accidental or intentional actions of internal employees
  - c. Failure to comply with security legislation such as Gramm-Leach-Bliley Act, HIPAA, California SB 1386 or PCI
2. **Damage to Data Integrity.**
  - a. Compromise of assets from a third party, business partner, eBusiness transaction, internet access, hackers or viruses
  - b. Accidental or intentional actions of internal employees
  - c. Failure to comply with SOX
3. **Data Unavailability Due to *Force Majeure* or Other Actions of Man.**
  - a. Act of nature (snow, hurricane, flood, earthquake, etc.)
  - b. Accident and/or intentional man-made damage (toxic spell, fire, terrorism, hacker, virus, etc.)

### B. Mitigation Approaches

The design and management of an organization’s technical infrastructure requires a basic understanding of the location of the highest value assets—customer data, personally identifiable information, financial information, proprietary data, etc.—and the building of applicable controls for the technology around them. Deployment of technical controls also requires an understanding of network topology, hardware components, data flow, servers, network paths, applications and data. Picture them as layers surrounding the entire organization—physical facility, computer systems (network, applications, databases and operating systems), processes and people.

Numerous and diverse technical security options are available, and your organization’s requirements for a particular solution will vary based upon your size, complexity and risk appetite. Always beware of claims regarding a silver bullet (“*This gadget will make you SOX compliant!*”). No single technology can provide full protection. Always remember that technology is only as effective as the individuals who manage it.

At a minimum, establish the following security controls:

1. **Require Appropriate Security Controls throughout System Development Lifecycle.** This includes analysis, design, development, acquisition, testing, implementation, maintenance, enhancement and disposal.
2. **Protect Technology from Destructive Software.** Such as viruses and malicious codes that corrupt and/or impair normal operations.
3. **Implement Access Controls Based on Principle of Least Privilege** that support the segregation of duties.
4. **Include Information Backup, Replication and Recovery Procedures in the Business Continuity Plan (BCP).**
5. **Protect External Networks by Implementing Alerts to Anomalies and/or Unauthorized Access.**
6. **Practice Change Control and Configuration Management Processes.** Ensure only authorized updates, changes and approved configurations are implemented into your corporate technology environment.

## X. Future Actions

The objective of this paper is to underscore the risks associated with poor security practices. Regulations and liability do not discriminate based on the size of an organization. The exposure to adverse events, and the magnitude of them, will vary by incident; corresponding harm can severely damage businesses of any size. When addressed individually the variety and volume of potential occurrences can be daunting to prepare for. However, the establishment of basic policies and procedures can minimize the impact to an organization's operations and reduce the likelihood of adverse events. The establishment of information security rules for people, processes and technology has been mandated by regulators, and has become one of the costs of operating a successful business in today's market.

The mitigation approaches presented here highlight the key objectives of a successful security program. They can be used to facilitate planning as well as to validate an existing program. The approaches do not represent a comprehensive list that will guarantee regulatory compliance, but they will move an organization in the right direction. Your management team can employ the suggested mitigation approaches as a technique to stimulate discussion and to justify activities related to secure operations.

One of the objectives of an organization's management team is to set the information security direction and to recognize that it will take time to implement the necessary measures for risk reduction. Your organization should identify its highest risks and mitigate the top risks first. Managers should then assess the remaining risks to determine which are second most critical and mitigate them, and so on, to continue to reduce the threats to the company.

Probably the most difficult and expensive part of any risk mitigation program is the implementation of technology to effectively execute information security policies. An ounce of prevention, and successful planning, can go a long way toward alleviating the time and cost of implementation. The best approach is to establish team(s) to represent each business function. Security is not the sole domain of IT; it is the responsibility of the whole organization. It is important to create a culture in which your personnel are both educated and actively involved in reducing the risks to your organization.

## XI. Glossary

Term	Definition
Acceptable Use Policy (AUP)	Also known as Acceptable <u>Usage</u> Policy, an AUP is integral to the framework of information security policies. Companies often ask new hires to sign AUPs before granting them access to their information systems. AUPs must be clear, concise, include the most critical rules about how users should use the corporate information technology and infrastructure, and include the penalties for noncompliance.
Authentication Factor	A piece of information, and a process, used to authenticate or verify a person's identity for security purposes.
Content-Filtering Web Proxy	Can support authentication to control access to the Web. It usually produces logs, either to give detailed information about the URLs accessed by specific users, or to monitor bandwidth usage statistics. It can also be used to provide security against viruses and other malware by scanning incoming content in real time before it enters the network.
Crimeware	Software designed to perpetrate identity theft, in order to access a computer user's online accounts at financial service companies and online retailers, for the purpose of stealing funds or completing unauthorized transactions. Crimeware exports confidential or sensitive information from a network for financial exploitation.
Data Link Connection Identifier (DLCI)	Used with frame relay. A Data Link Connection Identifier (DLCI) is a channel number that is attached to frame relay data frames in order to tell the network how to route the data. This 10-bit field defines the destination address of a packet. In frame relay, only one frame can be transmitted at a time, but many logical connections can co-exist on a single physical line. The DLCI allows the data to be logically tied to one of the connections so that once it gets to the network; it knows where to send it.
Federal Financial Institutions Examination Council (FFIEC)	Formal U.S. government interagency body empowered to prescribe uniform principles, standards and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS). It also makes recommendations to promote uniformity in the supervision of financial institutions.
Freeware	Computer software that is available for use at no cost or for an optional fee. Since freeware refers to the terms under which software is provided, it is a type of software license rather than a functional software category. It is <i>not</i> the same thing as free software.
Harassing Website	Whereas content can be offensive in a non-specific way, harassment directs obscenities and derogatory comments at specific individuals focusing, for example, on gender, race, religion, nationality or sexual orientation. Harassment often occurs in chat rooms, through newsgroups, and by sending hate email to targeted parties.
Identity Control	?
Malicious Website	?

Multi-Factor	According to the FFIEC in 2006, "by definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category ... would not constitute multifactor authentication."
Passphrase	A sequence of words or other text used to control access to a computer system, program or data. A passphrase is similar to a password in usage, but is generally longer for additional security.
Principle of Least Privilege	Also referred to as "least user access" or "least-privileged user account" (LUA), it is the concept that all users at all times should run systems with as few privileges as possible, and also be able to launch applications with as few privileges as possible.
Public/Private Keys	?
Spam	Unsolicited bulk email, fraudulent email, email in which the sender's identity is forged, or email sent through unprotected SMTP servers, unauthorized proxies.
Spamming	The process of sending spam.
Spyware	Computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user's interaction with the computer without the user's informed consent.
Strong Authentication	The use of more than one authentication factor to authenticate or verify a person's identity.
Web Proxy	Web Proxy serves as a web cache to provide a means of denying access to certain URLs in a blacklist, thus providing content filtering.

## XII. References

### ***Mortgage Bankers Association (MBA):***

[MBA Security Resource Center](#)

[MISMO](#)

[Secure Identity Services Accreditation Corporation](#)

### ***MERS:***

<http://www.mersinc.org/>

### ***Legislation & Regulations:***

[FFIEC Information Technology Examination Handbook](#)

[FFIEC & FTC Red Flag Identity Theft Regulations](#)

[FTC GLB Act Safeguard Rules](#)

[FTC Identity Theft](#)

[FBI Financial Crimes Report](#)

[National Conference of State Legislatures \(NCSL\)](#)

[CA Office of Privacy Protection](#)

### ***Policies & Best Practices:***

[National Institute of Standards & Technology \(NIST\)](#)

[American Institute of Certified Public Accountants \(AICPA\)](#)

[International Standards Organization \(ISO\)](#)

[Control Objectives for Information and related Technology \(COBIT\)](#)

[Committee of Sponsoring Organizations \(COSO\)](#)