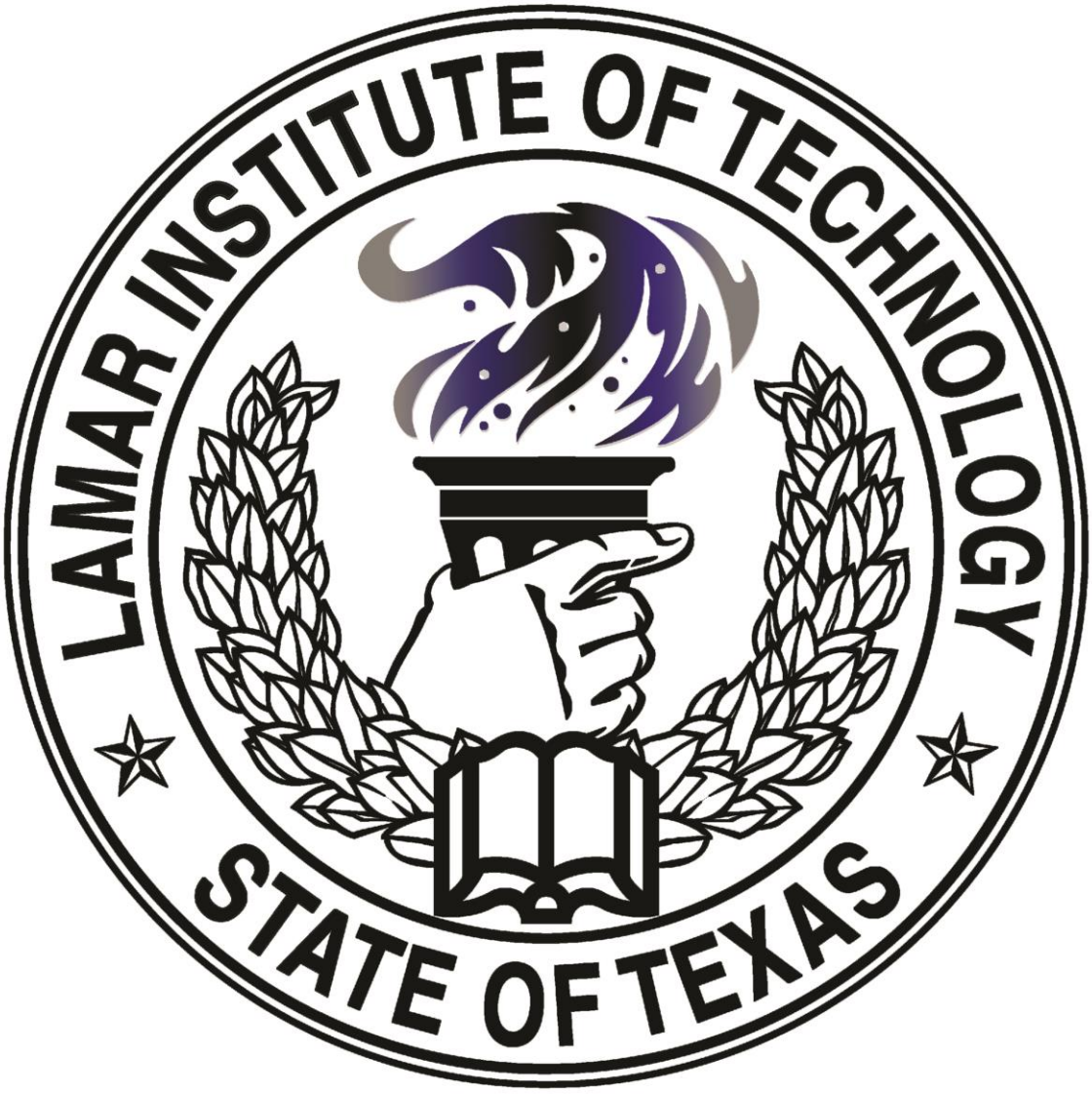
10/25/2012

TECHNOLOGY SERVICES

INFORMATION TECHNOLOGY RISK MANAGEMENT PLAN



Contents

Revision History

Revision Number	Version Date	Description of Changes	Changes Made By:
1.4	**2/25/11**	Included additions indicated by Isaac Barbosa. Methodology, Revision History, Activities	Cory Trahan
1.5	**3/16/11**	Included additions of risk (inherent and residual) and appropriate matrixes	Cory Trahan
1.6	**3/23/11**	Create Appendix sections A & B, Move Security and Red Flag Rules Programs into appendix	Isaac Barbosa Cory Trahan
1.7	**6/7/11**	Modify Appendix sections A and B. Created Appendix C. Removed parts of Risk Assessment from the main document.	Isaac Barbosa Cory Trahan Shawn Gallet
1.8	**6/16/11**	Created Appendix D, modified risk assessment in main document, inserted high-level workflow	Cory Trahan
1.9	**8/24/11**	Delete sections, organize and renumber appendices, expand on different sections	Isaac Barbosa
1.91	**9/19/11**	Delete and reorganize appendices, expand different sections.	Isaac Barbosa
	10/3/11	Delete footer content, adjust margins	Isaac Barbosa
2.0	**4/13/12**	Add policy development process, centrally managed resources, and consolidate and update appendices	Isaac Barbosa
2.01	**6/1/12**	Add the use of Identity Finder as part of the Security Awareness Program.	Isaac Barbosa
2.1	**10/25/12**	Added security reviews to Information Security Program Objectives and Activities	Isaac Barbosa

2.1	**2/19/13**	Make a few appropriate verbiage changes, move Policy Development and Centrally Managed Information Resources to Program Overview section	Isaac Barbosa
2.2	**2/25/13**	Grammar and verbiage changes, recommend Policy Development rewrite	Melissa Armentor
2.3	**10/1/14**	Periodic review	Isaac Barbosa
2.31	**10/29/14**	Document title change from Program to Plan, Begin adding procedures and procedure deliverable	Isaac Barbosa
2.31	**11/24/14**	Approved by President's Council	President's Council

Lamar Institute of Technology (LIT) has established a holistic approach to information technology (IT) risk management. Risk is the foundation to policy and procedure development. Once policies and procedure are in place, policy life-cycle management will ensure properly managed assets. The authoritative foundation for this program is Title 1, Part 10, Chapter 202, Texas Administrative Code, commonly known as TAC 202, and The TSUS Rules and Regulations Chapter III, Paragraph 19.

The program will provide a list of key strategies to follow to utilize information resources to further the mission of Lamar Institute of Technology (LIT) and to create an institution-wide security aware culture as well as initiate executive leadership support in the form of policies and governance.

Purpose

The purpose of this risk management program is to conduct appropriate activities to mitigate risks associated with information resources. The program will identify areas of risk considered as sensitive and requiring monitoring on an on-going basis. Stakeholders will properly document this monitoring, in the form of risk assessment activities.

Program Overview

LIT has a methodology for addressing risk. This methodology defines processes that will appropriately mitigate risk at LIT. This methodology is ever evolving and annual assessment will effectively mitigate risk.

Policy Development

Policy development and the resulting policies are the foundation allowing the success of this program. All policies at LIT must be developed through, and approved by President's Council and are published in the LIT Policies and Procedures Manual.

Centrally Managed Information Resources

Established information resource policies dictate that the Technology Services department under the direction of the Information Resource Manager (IRM) centrally manages information resources. These resources are assets acquired, managed, and retired appropriately in order to maintain standards and comply with established mandates and guidelines. The IRM will approve all IT purchases in order to maintain information resource standards. In addition, the IRM will ensure that all assets are properly retired according to State guidelines.

Program Methodology

Risk is the foundation on which LIT develops IT policies. Stakeholders will analyze areas of risk and develop activities to mitigate those risks. Those activities may include developing policies and procedures.

Life-Cycle management is the key to ensuring risk mitigation is an on-going practice. Life-cycle management applies to, and is not limited to employees, students, constituents, information resources, policies, and procedures. LIT will identify processes necessary to ensure all life cycles are appropriately managed.

The LIT Information Resource Manager (IRM) will manage the Risk Management Program and take an active role in managing IT risk at LIT.

Stakeholders

Stakeholders include and are not limited to:

- Employees
- Students
- Constituents
- Vendors
- Contractors

Areas of Risk

Identified areas of risk include and are not limited to:

- Physical and digital information resources
- Server and computing environments
- Networks

These major areas can further be broken down to the following detail areas:

- Access Control
- Application Development
- Business Continuity/Disaster Recovery
- Data Safeguards
- Information Security Governance and Risk Management
- Compliance Legality and Regulations
- Operation and Physical Security
- Telecommunications and Networking

Framework Phases

- Strategic Risk Assessment Planning
- Operational Data Collection
- Risk Analysis
- Mitigation Planning (Repeat to Phase 1)

Lamar Institute of Technology will also coordinate with the Office of Audits and Analysis to identify risk.

Program Specifics

Lamar Institute of Technology recognizes risk management is a holistic and ongoing process institution wide. It is the responsibility of every employee and based on risk self-assessment at every level of the organization. Processes will be identified and evaluated for potential risks, impact, probability, and mitigating controls.

The risk assessment team uses a management-facilitated workshop to brainstorm and identify all possible processes and/or activities. Interviews and available tools will obtain what risks exist. Mitigating activities may take the form of policies and procedures put into place by management to mitigate identified risks.

Program Activities

For each area of identified risk, LIT will appoint a team of stakeholders responsible for conducting a self-analysis in the identified area of risk. The process will include but is not limited to conducting interviews with stakeholder constituent groups, running appropriate reports, testing processes and procedures, reviewing policies, and other relevant activities to demonstrate due diligence in identifying and mitigating risk. In addition, the team will exercise due diligence in identifying and recommending appropriate policies, procedures, and/or other activities to mitigate identified risks.

Qualitative Risk Assessment

There are formulas for Inherent Risk and Residual Risk. ***Inherent risk*** is raw risk present and not taking into consideration any mitigating controls. An example of inherent risk would be a virus attack that may have a high Impact and a high likelihood if no controls existed. ***Residual risk*** is the likelihood and impact the risk will have when considering the mitigating controls. There may still be a high impact, but the likelihood is low. If you were able to mitigate the impact then you may get residual risk. Every risk assessment will consider both inherent and residual risk in developing a corrective action plan.

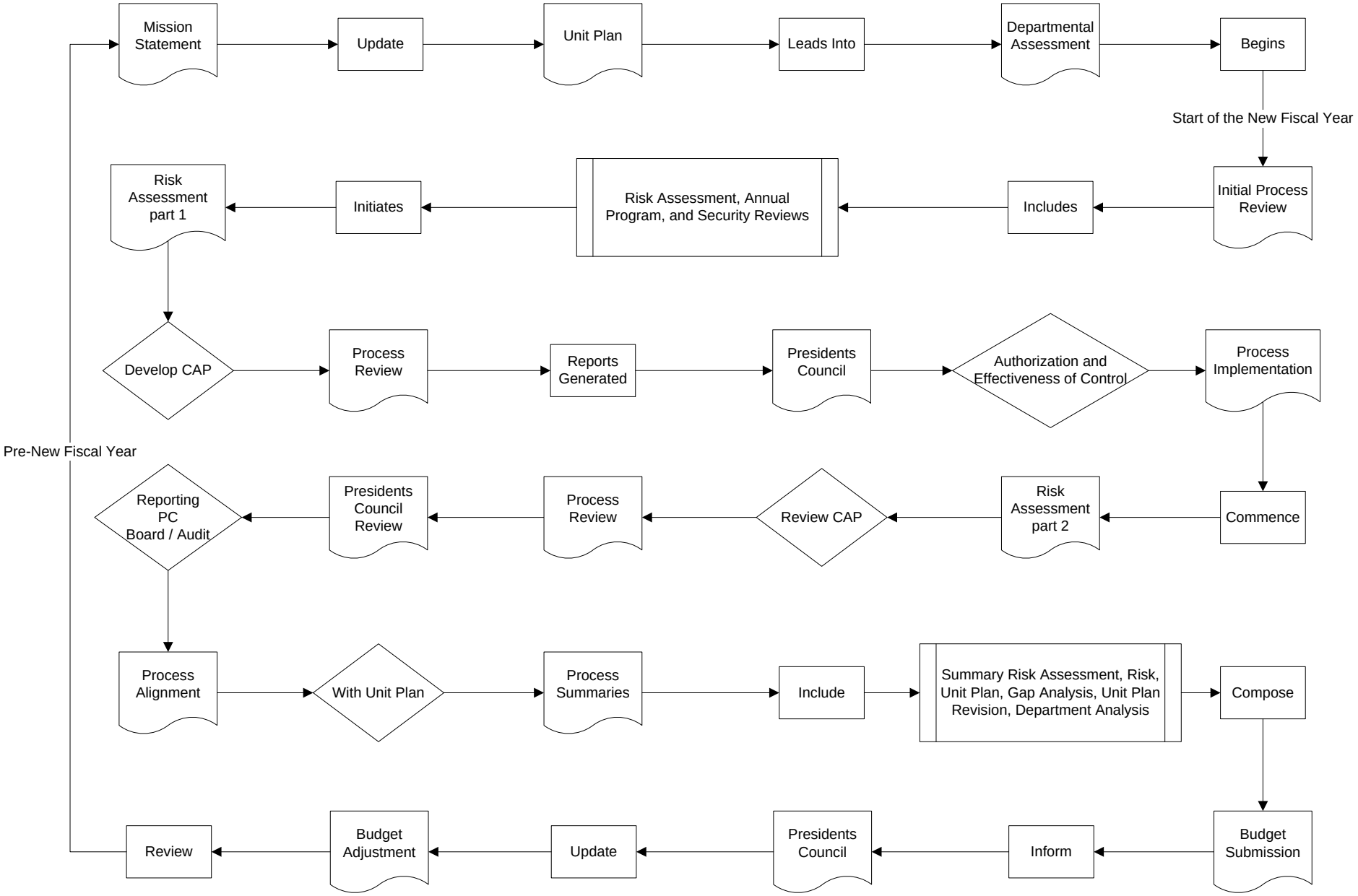
Mitigating Activities

LIT will develop and document activities associated with mitigating risk. These activities include but are not limited to implementing application programs, reviewing security logs and reports, and conducting penetration testing and vulnerability scanning. The collective of these activities will be considered a Threat Management Program managed by the LIT IRM.

Perpetual Evaluation

All programs have a life cycle monitored by the LIT IRM. Initial evaluation consists of a clear objective, identified areas of risk with ideas to mitigate the risk, any policies currently related to the objective, and an additional assortment of evaluation techniques such as a risk assessment matrix. At the appropriate designated time decided upon in the initial phase, a second evaluation will be conducted. This consists of evaluating dates, goals, and appropriate corrective action plans. The final evaluation goes to president's council and the office of internal audit and analysis in the form of a report to management.

High Level Annual Work Flow



Administration of the Program

LIT has designated the Director of Computer Services and Chief Information Officer (CIO) to be the program administrator. The CIO is responsible for implementing program policies, insuring that procedures are established and maintained, assigning responsibility and accountability, periodically reassessing operations and/or recommending program modifications, generating periodic status reports, and reporting annually to the Board of Regents' committee on the effectiveness of the Risk Management Program.

Appendix A – Information Security Program

Purpose and Scope

All members of the LIT community, regardless of position or role, share responsibility for protecting the information resources. The LIT community shall respond appropriately to protect information resources against accidental or unauthorized disclosure, contamination, modification, or destruction, and to assure the confidentiality, authenticity, utility, integrity, and availability of information.

Objectives

The objective of the information security program is implementing security and awareness, developing a methodology for assessing security in all areas, establishing security standards and reports and ensuring data security reviews in a timely manner.

Activities

Technology Services will perform a variety of activities on an ongoing basis as a part of the Information Security Program to ensure end users are aware of the security program and risks. These include but are not limited to:

- Risk Assessment
- Training
- Running Identity Finder
- Seminars and workshops
- Technology Services informative communications
- Security reviews

Identified Areas of Risk

To provide guidance to stakeholders, the identify areas are a starting point for the basis of an effective risk management program. The following are areas of risk:

Project Management

Project management practices are the cornerstone to successful implementation of any size project. LIT has designated the LIT IRM and the primary project manager for all IT projects. It is the responsibility of the IRM to insure that all projects follow project management best practices to ensure that all projects are properly planned; inherent to that planning is risk management.

Procedures:

All projects will be subject to the development of a project definition document that will contain project goals and measurable objectives to evaluate the successfulness of the project. The following checklist will provide guidance for all projects.

Project Quality Assurance Checklist:

- Defined goals and measurable objectives
- Proper funding with State or Local funds
- Vendor evaluation matrix
- HUB opportunities considered
- Identify project risks
- Policy considerations

Deliverable:

- An appropriate project plan and associated project checklist
- Identified risks section in project plan
- Identified risk mitigating activities if appropriate

Access Control

The following areas are areas where access controls should exist:

- System Administration
- Applications
- Networks
- Files
- Directories
- Data

Procedures

Regular reviews of the following institutional assets:

- ERP servers
- Data center servers
- Institutional computers
- Network accounts

Deliverable:

- Server review logs and administrator approvals
- Shared directory access logs and owner approvals

Application Development

The following are areas of risk in the area of application development:

- Application development process
- Testing
- Change management
- Data integrity
- Data loss

Procedures:

Changes to the following system will be documented and approved:

- Website changes
- ERP system changes

Deliverable:

- System owner approvals

Data Safeguards

Data safeguards are extremely critical areas needing analysis:

- Data Transfer
- Data integrity
- Data confidentiality
- Data storage media

Procedures:

- Off-Line storage media log review
- Surplus hard drive logs will be reviewed and properly disposed

Information Security Governance and Risk Management

The following have been identified:

- IT policies
- IT procedures

- Incident management
- Training
- Risk analysis

Procedures:

LIT security coordinators will provide security reports to the data owners annually for review. Those reports will take the form of Class Reports and associated objects and users that have access to those classes. Each data owner will review and approve the classes with their respective forms, and they will approve any users that have access to their forms in those associated classes.

Data owners will review security profiles annually at the direction of the LIT Information Resource Manager.

Deliverable:

- Approved security reviews annually

Compliance Legality and Regulations

Laws and regulations applying to LIT

- TSUS System guidelines
- State regulations
- Federal regulations
- FERPA, GLBA, ECPA/CFAA, State Breach laws, PATRIOT act, HIPPA, PCI

Operation and Physical Security

Physical access to information technology assets is a risk. The following areas have been identified:

- Desktop computer access
- Laptop access
- Data center access
- Removable media access
- Data network closets

Telecommunications and Networks

The network-computing environment is a risk. The following areas of risk have been identified:

- Viruses and related threats
- Hackers
- Firewalls and equipment

- IP phone system
- Traffic monitoring

Data Classifications and Definitions

Confidential Data

Laws:

- FERPA, GLBA, ECPA/CFAA, State Breach laws, PATRIOT act, HIPPA, PCI

Examples:

- SSN
- Credit Card Numbers
- Financial Records
- Records Information
- Clinical Information
- Personal vehicle license/registration information
- Employee record
- Student Grade Records
- Student Transcripts
- Access device numbers and passwords

Institutional Data (Sensitive Data)

Laws:

- Civil statute and regulation
- Freedom of Information Act
- Law enforcement investigation

Examples:

- ID Card photographs
- Lists of employees
- Emails containing sensitive information
- Electronic email addresses
- Tenure files
- DOB for employees and students
- Internal audit data

- Student evaluations
- Internal investigations

Public Data

Laws:

- Data is subject to disclosure to all employees as well as general public
- FERPA, HIPCA,

Examples:

- Website
- Library data and holdings
- Public phone directory
- Course catalog and curriculum information
- Enrollment figures
- State budget
- All other public information

Responsibilities and Accountability for Confidential Data

The following roles have been defined:

Data Owner

The owner or his or her designated representative(s) are responsible for and authorized to:

- Approve access and formally assign custody of an information resources asset.
- Determine the asset's value.
- Specify data control requirements and convey them to users and custodians.
- Specify appropriate controls, based on a risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources and services outsourced by the institution of higher education.
- Confirm that controls are in place to ensure the confidentiality, integrity, and availability of data and other assigned information resources.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
- Review access lists based on documented security risk management decisions.

- Approve, justify, document, and be accountable for exceptions to security controls. The information owner shall coordinate exceptions to security controls with the information security officer or other person(s) designated by the state institution of higher education head.
- The information owner, with the concurrence of the institution of higher education head or his or her designated representative(s), is responsible for classifying business functional information.

Data Custodian

Custodians of information resources, including third party entities providing outsourced information resources services to state institutions of higher education shall:

- Implement the controls specified by the information owner(s);
- Provide physical, technical, and procedural safeguards for the information resources;
- Assist information owners in evaluating the cost-effectiveness of controls and monitoring; and
- Implement monitoring techniques and procedures for detecting, reporting, and investigating incidents.

Data User

Users of information resources shall use the resources only for defined purposes and comply with established controls and policies

Appendix B - Red Flags Rule Program

Purpose and Scope

In its capacity as a creditor, Lamar Institute of Technology (LIT) is subject to "Identity Theft Rules," which requires the establishment of a written Identity Theft Prevention Program for covered accounts. To protect existing consumers, reduce risk from identity fraud, and minimize potential damage from fraudulent account activities with the least possible impact on business operations, LIT establishes this Identity Theft Prevention Program.

The handlings of consumer accounts involving multiple payments are also in the scope of this program. Examples include but are not limited to the federal Perkins Loan Program; the federal Family Education Loan Program; Institutional loan programs for students, faculty, or staff; and Institutional tuition (or fee) installment payment plans.

Objective

Ensuring proper controls are in place to appropriately secure financial transactions and procedures.

Policy

Appropriate Use of Information Technology Policy
Information Security Policy

Definitions

Covered Account

- Bank accounts
- Credit card accounts
- Student accounts
- Vendor accounts
- Consumer Accounts

Identity Theft

- Fraud committed using the identifying information of another person.

Personally Identifiable Information

- Driver's license
- Social Security Number
- Birth date
- Spousal information

- 1098Ts
- W2s

Red Flag

- A pattern, practice, or specific activity indicating the possible existence of identity theft

Identification and Detection of Red Flags

LIT recognizes the following types of notices, documents, personal information, and activities may be indicators or red flags that an individual's identity may be compromised:

- Alerts, Notifications, or Warnings from a Consumer Reporting Agency
    - A fraud or credit alert is included with a consumer report.
    - A notice of credit freeze on a consumer report is provided from a consumer-reporting agency.
    - A consumer report agency provides a notice of address discrepancy.
    - A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a customer.
- Suspicious Documents
    - Documents provided for identification appear to have been altered or forged.
    - The photograph and/or physical description on the identification is not consistent with the appearance of the customer presenting the identification.
    - Other information on the identification is not consistent with information provided by the person opening an account or presenting the identification.
    - Other information on the identification is not consistent with readily accessible information that is on file with LIT.
    - An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Suspicious Personal Identifying Information
    - Personal identifying information provided is not consistent with external information sources used by LIT.
    - Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
    - Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third party sources used by LIT.
    - The social security number provided is the same as that submitted by other persons opening an account or other customers.
    - The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or to other customers.

  - The person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
  - Personal identifying information provided is not consistent with personal identifying information that is on file with LIT.
  - If LIT uses a challenge question, the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- Compromised Systems
  - Detection of compromised or breached systems storing covered accounts or personally identifiable information.

Responding to Red Flags

- LIT will respond appropriately to identified and detected red flags in order to prevent and mitigate identity theft. The response shall be commensurate with the degree of risk posed.
- Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and LIT from damages and loss.
- Each unit based upon business and technical needs must maintain approved standards and responsive action. Administration recommends the following responses to red flags:
  - Alert and involve a business unit manager;
  - Notify designated LIT official;
  - Monitor a covered account for evidence of identity theft;
  - Where appropriate, change any passwords, security codes, or other security devices;
  - Close an existing covered account;
  - Reopen a covered account with a new account number if needed;
  - Contact customer;
  - Request additional documentation to validate identity;
  - Handle per regulatory requirements under law if applicable;
  - Handle per applicable Institutional privacy and information security policies, as noted in Section 3;
  - Notify law enforcement or regulatory entity; or
  - Determine no response is warranted under the particular circumstances.

Appendix C - Security Awareness Program

Purpose and Scope

Lamar Institute of Technology (LIT) realizes the importance of State, Institutional, and Constituent information resources and is dedicated to protect these assets against unauthorized access, disclosure, modification or destruction. To assure the availability, integrity, utility, authenticity, and confidentiality of information resources, LIT has adopted this security awareness program that will provide opportunities to make users aware of security risks inherent to daily operations. The core of this program consists of New Employee training; Roles, Responsibilities, and Data Classification training; and Identity Theft Protection training.

New Employee training is required of all incoming employees. Roles, Responsibilities, and Data Classification training is provided to all employees that have been identified as having access to information that is confidential in nature. Identity Theft Protection training is provided to employees that have access to information that provides identity theft opportunities. Training will be documented and verified through the use of quizzes designed to insure that the training has been completed.

As indicated on the LIT Administrative Systems Account request form completed by all employees and their supervisor, each supervisor is to be aware of the level of access their employees have to information resources. This program requires that each supervisor identify the appropriate training required for each of their employees. In addition, each supervisor is to identify the frequency of the training required for their employees. Not all employees have the same level of access to information resources and the risk of compromising information resources is not the same for all employees.

The security program also provides for the regular review of information security to insure that user access if appropriate for appointed duties and responsibilities. The security reviews will include both application and database access by both users and system processes. Process accounts will be managed in a way that will insure that access to those process accounts are used appropriately. Security reviews will be documented and maintained through the office of the Director of Computer Services.

Additional opportunities are provided in the form of email notifications, training sessions, and presentations.

This Security Awareness Program identifies detailed activities that are in support of the LIT Risk Management Plan and associated programs.

Responsibilities of Users

- Each user shall utilize LIT information resources responsibly and respect the needs of other users.
- Each person is responsible for any usage of his or her LIT ID. Users must maintain the confidentiality of their passwords.
- A user must report any abuse or misuse of information resources or violations of any information resource policy to their department head or to the Director of Computer Services.
- Each supervisor is responsible for coordinating end user training with their supervisor and the Technology Services Help Desk.

End User Training

- Appropriate Use of Information Technology
  - Training Quiz
- Roles, Responsibilities, and Data Classification
  - Training Quiz
- Identity Theft Protection
  - Training Quiz

Security Reviews

- Elevated Account Reviews
  - Daily Account Review
- Banner Class Reviews
  - Annual Class Review
- Banner User Reviews
  - Annual User Access Review

- Network Access Reviews
    - Annual User Access Reviews
- Server Access Reviews
    - Annual User Access Reviews

Security Tools

LIT will establish and employ a standard tool set in support of the security awareness program. These tools will be in the form of hardware, software, and reports.

Information Security Reviews

In order to effectively manage and mitigate risk, LIT will conduct regular reviews of information resources.

Banner Security Reviews

- User Account Reviews
- Elevated Account Reviews

Data Center Reviews

- Server Reviews
- Departmental Share Reviews
- Active Directory Account Reviews
- Identity Finder Scan Reviews
- Server Monitoring Reviews
- Virtual Environment Monitoring Reviews
- Storage Environment Monitoring
- Email Filtering and Monitoring

Network Security Reviews

- Intrusion Detection
- Firewall Configuration Reviews
- Network Access Reviews
- Virtual Private Network Configuration Reviews
- Network Host and Services Reviews
- Network Traffic Reviews