REPORT TO MANAGEMENT ON

REVIEW OF DISASTER RECOVERY PLAN

LAMAR INSTITUTE OF TECHNOLOGY

DECEMBER 2002
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRANSMITTAL LETTER</td>
<td>3</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>5</td>
</tr>
<tr>
<td>DETAILED FINDINGS AND RECOMMENDATIONS</td>
<td>9</td>
</tr>
</tbody>
</table>
December 11, 2002

Dr. Robert Krienke, President
Lamar Institute of Technology
P.O. Box 10043
Beaumont, TX 77710

Dear Dr. Krienke:

Enclosed is the audit report entitled, **Report to Management on Review of Disaster Recovery Plan, December 2002**. The objective was to assess if Lamar Institute of Technology has a business continuation plan for any minor or major disaster that may occur. Also, Internal Audit selected to review the Computer Services Department’s disaster recovery plan, which is a sub-component of the business continuation plan, to ensure the department is prepared to resume telecommunications or information system resources in a timely manner. Our examinations were based on questionnaires and supporting documents.

Lamar Institute of Technology does not have a business continuation plan to cover all business functions of its campus and business management responsibilities. The Institute did not comply with the Texas Administrative Code, Title 1, Part 10, Rule 202.6 which states each agency should approve and maintain a written business continuation plan, distribute it to key personnel, and store a copy of the plan at its designated off-site facility. It is the responsibility of the agency head to approve the plan.

Also, the Computer Services Department does not have a disaster recovery plan. Lamar Institute of Technology has an inter-agency contract with Lamar University that develops and maintains the Institute’s Financial Records System, Human Resource System, and Student Information System. The department did not comply with the Texas Administrative Code, Title 1, Part 10, Rule 202.6 which states key elements of the information resources plan should include:

- a business impact analysis;
- a security risk assessment;
- a recovery strategy;
- an implementation, testing, and maintenance management program; and
- a written disaster recovery plan to:
  - address the impact and magnitude of loss or harm that will result from an
interruption;
• identify recovery resources and a source for each;
• list step-by-step instructions for implementing the plan;
• maintain currency; and
• test at least annually.
• a mission critical data backup schedule.

Finally, Internal Audit noted the Computer Services Department’s responses from the questionnaires did not accurately reflect supporting documents.

Without a detailed plan for implementation and recovery planning, the risk exists that the Institute may be unable to continue critical day-to-day operations. Also, the Computer Services Department may not be able to restore, in a timely manner, critical information systems that provide vital business functions and to manage the availability of information systems data and resources in the event of a processing disruption. The department may not be able to receive assistance from its off-site or alternate facility, hardware and software support from vendors, or meet the computing needs of its faculty, staff, and students. Finally, the department does not have its contractual or written agreements with vendors or other institutions in the plan to specify the responsibilities of both parties or the level of support they would provide.

Based on criteria prescribed by the Rules and Regulations of The Texas State University System, the audit is a Category II.

We appreciate the cooperation received from management and the Computer Services Department during our audit. If you should have comments or questions, I am available at your convenience to review the report.

Sincerely,

Twila J. Baker
Director of Internal Audit
OBJECTIVES

The Internal Audit Plan for fiscal year 2003 provides for a review of the disaster recovery plan. The objective was to determine if Lamar Institute of Technology has a business continuation plan for any minor or major disaster that may occur. Also, Internal Audit selected to review the Computer Services Department’s disaster recovery plan, which is a sub-component of the business continuation plan, to ensure the department is prepared to resume telecommunications or information system resources in a timely manner. Our examinations were based on questionnaires and supporting documents.

Based on criteria prescribed by the Rules and Regulations of the Texas State University System, the audit is a Category II.

BACKGROUND

A business continuation plan is a process of developing and maintaining an effective written plan of how your organization will continue to operate in the event of an interruption, not only in the information systems or telecommunication areas, but also in other vital functions of an organization. Furthermore, the plan is designed to reduce the consequences of the loss of any telecommunications or information system resources or capabilities to an acceptable level. The planning process is not just a planned response to a major catastrophe but is custom-made around your organization’s business practices, hardware, and software.

RESULTS OF REVIEW

Lamar Institute of Technology does not have a business continuation plan to cover all business functions of its campus and business management responsibilities. The Institute did not comply with the Texas Administrative Code, Title 1, Part 10, Rule 202.6 which states each agency should approve and maintain a written business continuation plan, distribute it to key personnel, and store a copy of the plan at its designated off-site facility. It is the responsibility of the agency head to approve the plan.

Also, the Computer Services Department does not have a disaster recovery plan. Lamar Institute of Technology has an inter-agency contract with Lamar University that develops and maintains the Institute’s Financial Records System, Human Resource System, and Student Information System. The department did not comply with the Texas Administrative Code, Title 1, Part 10, Rule 202.6 which states key elements of the information resources plan should include:

- a business impact analysis to address maximum tolerable downtime for time-critical support services and resources;
- a security risk assessment to weigh the cost of implementing preventative measures against
the risk of loss from not taking action;
• a recovery strategy to appraise recovery alternatives and alternative cost-estimates;
• an implementation, testing, and maintenance program to address the initial and ongoing testing and maintenance activities of the plan;

• a written disaster recovery plan to:
  • address the impact and magnitude of loss or harm result from an interruption;
  • identify recovery resources and a source for each;
  • list step-by-step instructions for implementing the plan;
  • ensure currency; and
  • test at least annually.
• a mission critical data shall be backed up on a scheduled basis and stored off-site.

Finally, Internal Audit noted the Computer Services Department’s responses from the questionnaires did not accurately reflect supporting documents.

CONCLUDING REMARKS

Lamar Institute of Technology is not prepared should any minor or major disaster occur at the campus. The Institute should develop and store a copy of the plan at its designated off-site facility, so the Institute could resume its operation, if partial or all of the campus is deemed unusable for a period of time. The Computer Services Department should develop a disaster recovery plan to include the elements as stated in the Texas Administrative Code and include pertinent documentation in the plan. This will help ensure the department complies with the Code; provide the Institute the ability to continue their financial, administrative, and student services operations with minimal disruption; and protect vital data documents and records to minimize the susceptibility of a litigation.

Without a detailed plan for implementation and recovery planning, the risk exists that the Institute may be unable to continue critical day-to-day operations. Also, the Computer Services Department may not be able to restore, in a timely manner, critical information systems that provide vital business functions and to manage the availability of information systems data and resources in the event of a processing disruption. The department may not be able to receive assistance from its off-site or alternate facility, hardware and software support from vendors, or meet the computing needs of faculty, staff, and students. Finally, the department does not have its contractual or written agreements with vendors or other institutions in the plan to specify the responsibilities of both parties or the level of support they would provide.

We appreciate the assistance provided to Internal Audit by management and the Computer Services Department during the course of this audit.
REPORT TO MANAGEMENT ON
REVIEW OF DISASTER RECOVERY PLAN

LAMAR INSTITUTE OF TECHNOLOGY
DECEMBER 2002

Copies of this report have been mailed to the following:

Lamar Institute of Technology
Dr. Robert Krienke, President
Mr. Jonathan Wolfe, Vice President for Finance and Operations
Dr. Kenneth Shipper, Vice President for Instruction
Mr. Isaac Barbosa, Director of Computer Services

The Texas State University System
Mr. J. Wiley Thedford, Vice Chancellor for Finance
Mr. Jerry W. Neef, Director of Audits and Analysis

Project Auditors
Ms. Twila Baker, Project Director
Ms. Daphne McIntire, Project Auditor
DETAILED FINDINGS
AND
RECOMMENDATIONS

Review of Disaster Recovery
NONCOMPLIANCE TO THE TEXAS ADMINISTRATIVE CODE

Lamar Institute of Technology, as well as the Computer Services Department does not have a comprehensive plan to minimize the business impact and to ensure timely resumption of service in the event of a disaster or other disruption at the Institute.

The Texas Administrative Code (TAC), Title 1, Part 10, Rule 202.6 states an agency should maintain a written business continuation plan to cover all business functions of an agency and its business management responsibilities. The plan will minimize the effects of a disaster, and the agency will be able to either maintain or resume mission-critical functions. The agency head should approve the plan. The plan should be distributed to key personnel and a copy stored at an off-site facility.

Lamar Institute of Technology does not have a business continuation plan and did not comply with the Texas Administrative Code.

Lamar Institute of Technology heavily depends upon Lamar University’s Information Technologies Department to provide the Institute with the availability of computing to perform its financial, administrative, and student services systems. However, Lamar University does not assist the Institute with the availability of hardware and software support for its faculty, staff, and students; provide hard copy documents to continue its operations; or recover pertinent information on each individual microcomputer or computer lab. The Institute and the University should develop a written agreement specifying the level of support and responsibility the University would provide the Institute in the event the University’s computer facilities and equipment are unusable.

The Computer Services Department does not have a written disaster recovery plan that includes the following key elements as stated in the TAC:

- A business impact analysis to assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. Also, it should address maximum tolerable downtime for time-critical support services and resources including, but not limited to:
  - personnel;
  - facilities;
  - technology platforms (all computer systems);
  - software;
  - information resources security utilities;
  - data networks and equipment;
  - voice networks and equipment;
LAMAR INSTITUTE OF TECHNOLOGY
DETAILED FINDINGS AND RECOMMENDATIONS

• vital electronic records and/or data.
• a security risk assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.
• a recovery strategy to appraise recovery alternatives and alternative cost-estimates and present it to management.
• an implementation, testing, and maintenance management program to address the initial and ongoing testing and maintenance activities of the plan.
• a written disaster recovery plan to:
  • address the impact and magnitude of loss or harm result from an interruption;
  • identify recovery resources and a source for each;
  • list step-by-step instructions for implementing the plan;
  • maintain currency; and
  • test at least annually.
• a mission critical data should be backed up on a scheduled basis and stored offsite in a secure, environmentally safe, locked facility accessible only to authorized agency representatives.

Internal Audit noted the department’s responses from the internal control questionnaires did not accurately reflect supporting documents. The department stated that Lamar University supports the Institute’s information systems, computer systems, computer programming, and business continuity planning for those systems. According to the University Information Technologies Department’s responses, the department’s plan covers the following critical systems: the Financial Records System, the Human Resource System, and the Student Information System. The Information Technologies Department’s plan does not cover other information resources operations and telecommunication areas at the Institute.

Overall, the Institute needs to develop a business continuation plan, distribute it to key personnel, and store a copy of the plan at its designated off-site facility, so the Institute could resume its operation, in the event partial or all of the campus is deemed unusable for a period of time.

Also, the Computer Services Department needs to develop a disaster recovery plan to include key elements as stated in the Texas Administrative Code. This will help ensure the department comply with the Code; provide the Institute with the ability to continue their financial, administrative, and student services operations with minimal disruption; and protect vital data documents and records to minimize the susceptibility of a litigation. Furthermore, the department needs to include contractual or written agreements with vendors or other institutions to specify the responsibilities of both parties relative to availability of the hardware and software support from vendors or the use of its off-site or alternate facility.
Finally, the department needs to ensure its facility, as well as, the backup or off-site facility has adequate physical security controls to prevent intentional or accidental destruction of data. These controls should provide for preventive measures and for both the replacement of records that may be destroyed and the continuity of operations following major hardware or software failure.

**RECOMMENDATION**

We recommend the Institute develop a business continuation plan for the campus, distribute it to key personnel, and store a copy of the plan at its designated off-site facility.

**MANAGEMENT'S RESPONSE**

As of April 7, 2003, Lamar Institute of Technology has drafted a business continuation plan entitled, *Emergency Management Plan for Lamar Institute of Technology*. The plan is comprehensive and includes all functions and services identified as critical to the campus and business management. The plan further identifies the relationship between Lamar Institute of Technology and Lamar University, and insures continuation of operations in the event of a minor or major disaster.

The responsibilities of Lamar University with respect to business continuation of operations at Lamar Institute of Technology will be identified in a service level agreement that will be drafted and approved by September 1, 2003. That document will tie to the Inter Component Services Agreement.

The final *Emergency Management Plan for Lamar Institute of Technology* will be approved and distributed by September 1, 2003.

**RECOMMENDATION**

We recommend the Institute develop a written agreement with Lamar University and other institutions regarding the level of support and responsibility either campus would provide in the event of a disaster.

**MANAGEMENT'S RESPONSE**

As of March 11, 2003, Lamar Institute of Technology, Lamar University, Lamar State College-Orange, and Lamar State College-Port Arthur began meeting to develop written agreements that identify their coordinated efforts to insure business continuation at each campus. As appropriate, service level agreements will be drafted and approved by September 1, 2003.
Specifically, a service level agreement between Lamar Institute of Technology and Lamar University with respect to business continuation of operations at Lamar Institute of Technology will be drafted and approved by September 1, 2003. That document will tie to, or be a part of, the Inter Component Services Agreement.

**RECOMMENDATION**

We recommend the Computer Services Department develop a disaster recovery plan and include key elements as stated in the Texas Administrative Code, Title 1, Part 10, Rule 202.6.

**MANAGEMENT'S RESPONSE**

As of March 10, 2003, Lamar Institute of Technology Computer Services Department has drafted a disaster recovery plan that is in compliance with the Texas Administrative Code, Title 1, Part 10, Rule 202.6. The final document will be integrated into the final version of the *Emergency Management Plan for Lamar Institute of Technology* which will be adopted and distributed by September 1, 2003.

**RECOMMENDATION**

We recommend all departments develop a disaster recovery plan to protect their information resource assets and operating capability.

**MANAGEMENT'S RESPONSE**

As of April 7, 2003, the major functional areas that are critical to business continuation at Lamar Institute of Technology have been identified. By May 9, 2003, each functional area will receive assignments as to their responsibilities to document and develop a “unit plan” for emergency management.

Those unit plans will be completed by July 25, 2003.

**Business Continuation Plan Time Line**

<table>
<thead>
<tr>
<th>Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lamar Institute of Technology Computer Services Department draft Information Technology Disaster Recovery Plan. (Recommendation #3)</td>
<td>March 10, 2003</td>
</tr>
</tbody>
</table>
Lamar Institute of Technology, Lamar University, Lamar State College-Orange, and Lamar State College-Port Arthur begin developing inter component disaster recovery support agreements. (Recommendation #2)  
March 11, 2003

Lamar Institute of Technology draft a business continuation plan entitled, *Emergency Management Plan for Lamar Institute of Technology*. (Recommendation #1)  
April 7, 2003

All functional areas critical to operations of the campus and business management identified. (Recommendation #4)  
April 7, 2003

Assignments (unit plans) distributed to all functional areas identified as critical to operations and business management. (Recommendation #4)  
May 9, 2003

Unit Plans for all functional areas identified as critical to the campus and business management completed. (Recommendation #4)  
July 25, 2003

Service Level Agreement with Lamar University and their responsibility to Lamar Institute of Technology to insure business continuation of operations approved and signed. Other agreement approved and signed as appropriate. (Recommendation #2)  
September 1, 2003

Final *Emergency Management Plan for Lamar Institute of Technology* approved and distributed. (Recommendation #1)  
September 1, 2003

---

**Review of Disaster Recovery**