The College of New Jersey
Information Technology

July 1, 2005 to December 30, 2005

Richard L. Fair
State Auditor
The Honorable Jon S. Corzine  
Governor of New Jersey

The Honorable Richard J. Codey  
President of the Senate

The Honorable Joseph J. Roberts Jr.  
Speaker of the General Assembly

Mr. Albert Porrioni  
Executive Director  
Office of Legislative Services

Enclosed is our report on the audit of the The College of New Jersey, Information Technology for the period of July 1, 2005 to December 30, 2005. If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair  
State Auditor  
March 22, 2006
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>1</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Network Security</td>
<td>3</td>
</tr>
<tr>
<td>Change Management</td>
<td>3</td>
</tr>
<tr>
<td>Disaster Recovery and Business Continuity</td>
<td>4</td>
</tr>
<tr>
<td>IT Asset Disposal Process</td>
<td>5</td>
</tr>
<tr>
<td>Auditee’s Response</td>
<td>7</td>
</tr>
</tbody>
</table>
The College of New Jersey
Information Technology

Scope

We assessed network vulnerability and reviewed the adequacy of Information Technology (IT) policies and procedures for The College of New Jersey (TCNJ) for the period July 1, 2005 to December 30, 2005. Our audit evaluated selected controls in place over the college's network and systems that process and protect both public and private information. They are as follows:

- Business continuity plans in the event of processing interruptions.
- Protection of college resources from unauthorized access, use, and alteration.
- Change control process.
- Physical and logical security in place to protect the college's IT infrastructure.
- IT strategic planning.

Objectives

The objectives of our audit were to determine the adequacy of controls over the computer network to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to ensure changes are properly implemented and documented, and to provide for adequate planning.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with Governmental Auditing Standards issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the Open Source Security Testing Methodology Manual issued by the Institute for
Security and Open Methodologies, benchmarks issued by the Center for Internet Security, and Control Objectives for Information and Related Technology (COBIT) issued by the IT Governance Institute.

In preparation for our testing, we studied legislation, college operation plans, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those requirements was verified by interview of key personnel, observation and access of network infrastructure, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

**Conclusions**

TCNJ management has recognized the importance of security over their network and the services it provides. The Network Administrators and support staff have done an admirable job of maintaining the college network and its connectivity given its complex nature. We found controls in place and functioning to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to ensure changes are properly implemented and documented, and to provide for adequate planning. However, we noted certain control weaknesses requiring management’s attention. We also have provided TCNJ with a management letter containing a more detailed discussion of network security specifics.
Network Security

The TCNJ network allows services over logical connections between several computers that are not necessary. Allowing these services increases the risk of unauthorized access and network disruption. These services should be shut down.

We also noted weaknesses with the security software update process for the network. This process should be improved.

We also found possible unauthorized extensions of student residential network services. TCNJ should amend their Computer Access Policy to specifically address the extensions in question.

Finally, we noted certain controls over specific servers that should be strengthened.

For each of these cases, we have provided the college with the necessary technical details.

Network administrators should turn off unnecessary services and regularly monitor the network to ensure none are improperly enabled in the future, institute procedures to assure all machines on the network have current security software, amend the Computer Access Policy to specifically address improper network extensions, and strengthen specific server controls.

Recommendation

The college does not have a written network change control procedure.

Change Management

The college has no written policy to provide guidance on initiation, authorization, development, testing, and migration of changes to the network. IT standards state that the implementation of changes should be controlled by the use of a formal change control procedure. This procedure should include identification and
recording, categorization and prioritization, planning and testing, formal approval procedures, communication to all parties, and fallback procedures. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures.

**Recommendation**

We recommend that the college develop and implement a written network change control procedure that is in accordance with accepted IT standards and includes the components listed above.

---

**Disaster Recovery and Business Continuity**

The college’s disaster recovery plan states that alternate site inventory and equipment acquired through vendors is considered to be the only resource with which to recover computer processing. In addition, it states that an alternate site (backup computer facility) in which to establish recovery of computer processing is necessary. The disaster recovery plan also assumes that the computer facilities of the alternate site will not be impacted by any disaster which may interrupt computer operations at the college’s offices. However, the college does not have a separate disaster recovery room completed for the server (non-mainframe) environment in operation. Back up servers are currently kept in the computer room with the production servers.

Our discussions with college personnel revealed that the disaster recovery site has been started but not completed. If a disaster were to occur, the lack of a completed and operational disaster recovery site would mean that processing operations may be unrecoverable until new machines are obtained and a new site is created to handle the operation. In addition, a disaster affecting the main computer room could destroy
both the back up servers as well as the production servers if they are maintained in the same room.

**Recommendation**

The college should complete the disaster recovery site as soon as possible, and move all back up servers and media to that location.

---

**IT Asset Disposal Process**

When a machine is removed from service at the college, it is donated, sold, or thrown out. If the machine is broken, it is placed in one of two bins located on campus, the hard drive is physically disabled, and the machine is stored until the college’s salvage vendor picks up the equipment. If the machine is still usable, it will either be donated to organizations with a need or picked up by a third party vendor which sells the machines on the college’s behalf. In all cases, the items are removed from the inventory system and the serial number and a brief description is recorded in a salvage database. We selected 20 machines from the salvage database and could not document the disposition of 18 items.

Industry standards and best practices state that an organization has an obligation to achieve and maintain an adequate protection of its assets. Our work determined that the college does not keep detailed records for the items that are removed from the inventory system. Though serial numbers are documented by the college when items are removed from inventory, there is no complete database containing pertinent information about the item and its final disposition, thus increasing the susceptibility of these items to misplacement or misappropriation.

**Recommendation**

The college should improve the audit trail for the disposal process by recording all pertinent information about items in the process, including
the final destination and disposition of the item. This information should be kept in one comprehensive database.
March 20, 2006

James B. Patterson
Assistant State Auditor
Office of Legislative Services
Office of the State Auditor
125 South Warren Street
PO Box 067
Trenton, NJ 08625-0067

RE: The College of New Jersey Information Technology Audit Report

Dear Mr. Patterson:

Enclosed are responses to the audit findings and recommendations outlined in The College of New Jersey Information Technology audit report relating to the audit performed for the period July 1, 2005 through December 30, 2005.

If your office requires additional information regarding the enclosed responses, please feel free to contact Nadine Stern, Chief Information Officer at (609) 771-3154.

Sincerely,

R. Barbara Gitenstein
President
Findings & Recommendations: Network Security

Management's Response

We are addressing the specific recommendations related to network security in the following ways:

- Two of the three service areas identified in the management letter will be shut down. We have reviewed the third area and determined that limited access is necessary to perform required business processes. We will limit access to essential services in this area. We will also continue to regularly monitor the network to ensure unnecessary services are not improperly enabled in the future.
- We have addressed the issues identified in the management letter, and additional procedures are in place to assure all machines on the network have current security software.
- The Computer Access Policy will be amended to address improper network extensions.
- We have already implemented some of the recommendations provided in the management letter related to specific server controls, and will implement the remaining recommendations shortly.

Findings & Recommendations: Change Management

Management's Response

There is an existing review process for network changes through the organization up to the director level. We will develop a written network change control procedure that documents these processes, and review IT standards as they relate to change management. We will prioritize and implement new procedures where appropriate and feasible.

Findings & Recommendations: Disaster Recovery and Business Continuity

Management's Response

We concur with this recommendation and work is continuing on the disaster recovery site.
Findings & Recommendations: IT Asset Disposal Process

Management’s Response

The IT asset disposal procedures have been revised, based on recommendations we received during the audit. We also acknowledge that other departments involved in the asset disposal process on campus need to revise their record keeping procedures. We will work with these areas to accomplish this.