Internal Audit has completed a review of the College of Engineering in conformity with the fiscal year 2005 audit plan. The objective of this review was to contribute to the improvement of risk management and the control systems within the College of Engineering by identifying and evaluating the college’s exposures to risks and the controls designed by management to reduce those risks.

BACKGROUND
Virginia Tech’s College of Engineering is the Commonwealth’s leading College of Engineering. The College, its faculty, and its administration are known in Virginia and throughout the nation for the excellence of its programs in engineering education, research, and public service. It is composed of a dozen departments with expenditures exceeding $100 million. The College has over 500 employees (including almost 300 faculty), 5,500 undergraduate students, and almost 2,000 graduate students.

The College is consistently rated as a premier institution by its peers in surveys of the nation’s engineering school deans by U.S. News & World Report. The magazine ranks both undergraduate and graduate programs in the top 35 in terms of quality. Also, the graduate program is ranked 16th in terms of reputation as reported by deans of other institutions.

The College ranks ninth in number of bachelor’s degrees awarded, 13th in master’s degrees, and 18th in Ph.D.’s. Virginia Tech’s College of Engineering is among the five largest schools of engineering in the country.

RISK EXPOSURE
Internal Audit periodically performs a detailed risk analysis of all of the university’s auditable entities using factors such as the amount of cash inflows, operating expenditures, grant activities, level of external regulation, etc. The goal of the process is to prioritize those entities within the university that should receive audit attention. The College of Engineering was determined to be a high risk entity due to the volume of research dollars associated with the college, health and safety issues and the operation of several service centers.

SCOPE
The scope included a review of grant administration, service centers, health and safety and network security. The review covered the period of July 1, 2003 to December 31, 2004.
OVERALL ASSESSMENT
Our review indicates that management has designed controls that are effective at reducing the college’s exposure to business risks, but some controls are not consistently applied. Improvements are recommended to achieve a fully effective system of internal controls. See attached appendices for recommendations and action plans.

MANAGEMENT:
Hassan Aref-Dean
Brad Martens-Director of Finance and Budget
Ed Nelson-Interim Assistant Dean for Administration
Glenda Scales-Associate Dean for Distance Learning and Computing

AUDITORS:
John Rudd-Director
Mel Bowles-Associate Director
Rachel Potters-Senior Auditor-In-Charge
Divya Amin-Senior Auditor
Linda Srygley – Senior IT Auditor

PC: Auditor of Public Accounts
Zack Adams
Ginger Clayton Allen
Hassan Aref
Kathy Atkins
Sara Barnett
Lee Bishop
Robert Broyden
Linda Bucy
David Clark
Ann Craig
Kathryn Dew
Wanda Foushee
O. Hayden Griffin, Jr.
Mike Harness
Amy Hill
Mary Hunter
James Hyatt
Dennis Kafura
Erdogan Kiran
William Knocke
Kurt Krause
Brad Martens
Mark McNamee
Ken Miller
Latrica Nell

Ed Nelson
Thomas Novak
Ishwar Puri
David Richardson
Dwight Shelton
Paul Siburt
Charles Steger
G. Don Taylor
Jim Thorp
Robert Walters
Margie Zelinski
Workstation and Server Security

Recommendation
Implement additional generally accepted, industry-standard guidelines for computer configuration and use, specifically:

- Empower information technology staff to implement security configuration changes to all computers in accordance with a College standard developed from generally accepted best practice documentation (see http://www.security.vt.edu)
- Tighten user account settings and management policies and add password protected screensavers and a login announcement that references the University Acceptable Use Policy
- Ensure that resources are adequate to secure and maintain computer equipment
- Apply UNIX patches and upgrades in a timely fashion
- Develop and implement an appropriate backup strategy for all user data.
- Implement procedures to ensure that separate accounts with limited privileges are utilized by end-users

Benefits/Basis
Implementation of additional security configuration settings will provide assurance that the data collected on servers and workstations is protected from unauthorized access and maintains a high degree of integrity.

Our review of servers and workstations within two departments indicated the following:

Chemical Engineering
- No proactive backup strategy for critical data
- Securely constructed passwords not required
- No password protected screen savers
- UNIX machine patches and updates are not installed in a timely fashion
- Responsibility for the root userid and password on the UNIX machines rests with a single graduate student with no assigned backup

Aerospace and Ocean Engineering
- Security settings on the Windows servers are not in accordance with university guidelines, www.computer.vt.edu/accounts_and_access
- Securely constructed passwords not required
- Hard copy maintenance logs are not kept to document critical changes made to servers
- Some staff are given full administrative privileges on machines

Management Action Plan
A College Information System and Security Policy is under development and will address the issues identified by Internal Audit with minor exceptions as addressed below. The document will be reviewed, discussed, and formally adopted by the Deans and Department Heads by August 2005.

Chemical Engineering
The department will strive to apply the most critical patches to UNIX servers as soon as practical and others at least once a semester.

Aerospace and Ocean Engineering
Some of the recommended settings on Windows Servers are in conflict with functionality requirements. The settings will be adopted whenever possible, and slightly relaxed where conflicts occur. Administrative rights are given to some users due to the requirements of some software which they need to get their work done. We will work to ensure that administrative privileges are granted only when necessary and will strive to minimize those situations whenever possible.

Risk Evaluation: High
Implementation Date: August 31, 2005
## Health & Safety: Inspection Reports

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a monitoring and follow-up system for Environmental Health and Safety Services (EHSS) inspection reports to ensure that fire safety, machine shop safety and lab inspection hazards noted on the reports are addressed formally and in a timely manner.</td>
<td>Formulation of a formal response and action plan for all hazards reported by EHSS would help mitigate the risk of personal injuries to students, faculty, and staff. Additionally, formal responses to inspection reports establish a thorough audit trail to document actions planned or completed.</td>
<td>The College will ensure that EHSS inspection reports are distributed to the Dept. Health and Safety Representative, the Dept. Head, and to the Dean, and that the date of receipt is clearly marked on those reports.</td>
</tr>
<tr>
<td>Review of fire inspection reports for four departments revealed several items that remain outstanding. Formal action plans were not documented.</td>
<td>Review of machine shop safety reports for two shops also revealed that recommendations have not been fully implemented and formal action plans were not documented.</td>
<td>The College will ensure that written action plans are developed for inspection reports within 60 days of receipt and that copies are distributed to the Lab or Shop Manager, the Dept. Head, and the Dean. This timeframe allows for scheduling maintenance and for ordering and installing materials. The College will request that EHSS review the action plans and provide Dept. Health and Safety Representatives a written assessment of their adequacy. When resources are not available to adequately address health and safety issues identified in future EHSS reports, the College will attempt to secure additional resources from the central administration.</td>
</tr>
<tr>
<td>Review of lab inspection reports for two departments revealed that health and safety representatives from the departments are not provided with the reports and an established follow-up procedure is not in place.</td>
<td></td>
<td>The College will ensure that action plans are developed and implemented for unresolved EHSS issues noted during the audit.</td>
</tr>
</tbody>
</table>

**Risk Evaluation: High**

**Implementation Date: August 31, 2005**
## Grant Administration

<table>
<thead>
<tr>
<th><strong>Recommendation</strong></th>
<th><strong>Benefits/Basis</strong></th>
<th><strong>Management Action Plan</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide additional training to both faculty and administrative personnel regarding expenditures charged to sponsored projects, focusing on federal grants expenditures and the regulations that apply to these grants. Encourage department heads and administrative personnel to more stringently review sponsored grant expenses and to consult with the Office of Sponsored Programs if they have any question regarding whether an expenditure is allowable. Where appropriate, work with the Office of Sponsored Programs to transfer unallowable expenditures on grants to a more appropriate source of funding.</td>
<td>Providing training and conducting thorough reviews of sponsored grant expenditures will help ensure that expenditures are appropriate and in compliance with both federal and university policies, thus avoiding potential fines and penalties. During our review of 40 grants we noted that nine grants contained expenditures that were unallowable. These expenditures were administrative supply expenses (office supplies, postage, etc) that are determined to be unallowable direct costs per federal Cost Accounting Standards outlined in university policy 3240: <em>Consistency in Charging Administrative and Clerical Costs</em>.</td>
<td>The College of Engineering (COE), through the Office of Sponsored Programs (OSP) will provide additional training to both faculty and administrative fiscal personnel regarding expenditures charged to sponsored projects, focusing on federal grants expenditures and the regulations that apply to these grants. The COE will reserve slots for its faculty and staff in the OSP training classes that are planned through Fall 2005; and encourage participation in those classes and the filling of those slots through e-mail announcements and through announcements at both Dept. Head Meetings and Fiscal Officers Meetings. OSP has already met with the College fiscal officers to explain their program to become a certified grants administrator. All fiscal officers in the College will be strongly encouraged to earn the certificate and to serve as instructors in the classes. An earned certificate may eventually be a preferred/required job qualification for fiscal positions within the College. Dept. Heads will be encouraged to support this initiative and to award employees who complete the training.</td>
</tr>
</tbody>
</table>

**Risk Evaluation:** Medium  
**Implementation Date:** November 30, 2005
Service Centers

Recommendation
Provide more specific direction and oversight to the college’s service centers.

Specifically:

- Ensure that service center rates are being reviewed in accordance with university policy.
- Develop periodic reports of service center activity for management review.
- Provide training to service center personnel regarding applicable university policies.
- Evaluate service centers with little or no activity to determine if it is beneficial to continue operating as a service center.

Benefits/Basis
Strengthening controls over service centers will ensure compliance with Policy 3250: Service Centers. Evaluating service centers with little or no activity will ensure that resources are being used efficiently and may help identify other underlying issues (i.e. unbilled recoveries).

Our review of five of the college’s service centers noted:
- Three centers had their rates rescinded by the Controller’s Office as the rates were outdated.
- Two centers were not splitting recoveries appropriately.
- One center was incorrectly charging expenses to the equipment reserve fund.
- Three centers had no cost recoveries for the current fiscal year, and unbilled activity was unknown.

More in-depth examinations were performed on two of the college’s service centers, revealing the following:
- One center had significant cost recoveries from external customers.
- One center had insufficient documentation to support customer charges.
- One center was not utilizing the Banner Accounts Receivable system for external billings and was not in compliance with funds handling guidelines.
- One center was not utilizing the appropriate account code for external recoveries.

Management Action Plan
Service Center rates will be examined yearly by the Dean’s Office during July to ensure that the rates have been reviewed by the Controller’s Office.

The Director of Finance for the College will develop periodic reports of service center activities. These reports will be reviewed quarterly by the assistant dean for administration beginning at the close of 1st quarter fiscal year 2006. The review of the service center activities will include determining whether or not it is beneficial for the center to continue operations. The Director of Finance will seek Internal Audit’s input during the development of these reports.

The Controller’s Office will be asked to provide yearly training/reviews for service center employees on applicable university policies. The Dean’s Office will request that this training be provided in October 2005 and continue every July. Special training will be requested for new service center employees. Additionally, service center employees will be reminded of applicable university policies through emails containing a link to the university’s policies webpage. These emails will be sent yearly.

Risk Evaluation: Medium
Implementation Date: Oct.31, 2005
**Disaster Recovery and Contingency Planning**

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform a risk analysis to determine and document which information resources are critical to efficient and effective departmental function. Develop and adopt an emergency response/disaster recovery plan that documents what measures will be taken now, or in the event of an emergency, to return those resources to service or to replace critical equipment and information. Store the document in a secure location for periodic reference and update it as needed or on an annual basis.</td>
<td>Identification of critical departmental resources and preliminary planning for the repair or replacement of those resources will help the department resume essential business processes in the event that an emergency or disaster occurs. The Departments of Aerospace and Ocean Engineering and Chemical Engineering have started their emergency response plans, however the plans are not complete and have not been approved by senior management.</td>
<td>A College Information System and Security Policy is under development and addresses these issues. This document will be reviewed and discussed by the Deans and Department Heads by August 2005. The College will implement an annual call for Disaster Recovery &amp; Contingency Plan from the System Administrators Council. There is currently a biennial Risk Analysis and Assessment conducted by the Information Systems Security Office which all departments have recently completed.</td>
</tr>
</tbody>
</table>

Guidance can be found at [http://security.vt.edu/playitsafe](http://security.vt.edu/playitsafe).

**Risk Evaluation:** Medium  
**Implementation Date:** August 31, 2005
TO: Finance and Audit Committee of the Board of Visitors
FROM: John C. Rudd, Director
DATE: May 6, 2005
SUBJECT: Audit Report – Capital Design & Construction

Internal Audit has completed a review of the Capital Design & Construction department, in conformity with the fiscal year 2005 audit plan. The objective of this review was to assess the effectiveness of the control systems designed by management to reduce the area’s exposures to key business risks impacting the processes outlined in the scope below.

BACKGROUND

Reporting to Bill Elvey, Assistant Vice President for Facilities, Capital Design and Construction is responsible for managing the process by which capital outlay projects are designed and constructed so as to maximize the program goals of the end users while effectively balancing each project's established parameters for cost, schedule, and quality. During the fiscal year 2003-2004, Capital Design & Construction managed the successful completion of seven projects ($67,939,860). During the same period, the department managed six projects that were under construction ($152,449,000) and five projects ($77,109,000) that were in some phase of design. Between 2001 to 2005, Capital Design and Construction successfully completed twenty projects with construction contracts that, in sum, totaled to $81,152,446. The total amount of change orders for those projects was $4,188,674 (equivalent to five percent of the original contract amounts).

RISK EXPOSURE

Internal Audit periodically performs a detailed risk analysis of all of the University’s auditable entities using factors such as the amount of cash inflows, operating expenditures, grant activities, level of external regulation, etc. The goal of the process is to prioritize those entities within the University that should receive audit attention. Capital Design and Construction was determined to be a medium risk entity due to the complexity and criticality of the projects that it manages.

SCOPE

The scope of the audit included the following functions: Design, Project and Change Order Management, Services Procurement, Environmental Health and Safety Training, Cost Management and Accounting, Network Security, Disaster Recovery and Contingency Planning, Software Configuration Management, and Website Management. The audit period was fiscal

OVERALL ASSESSMENT

Our review indicates that management has designed controls that are effective at reducing the department’s exposure to many of the business risks it faces, but some improvements are recommended to achieve a fully effective system of internal controls. Audit recommendations were issued to management where opportunities for further improvements were noted. See the attached appendices for our recommendations and management’s action plans.

MANAGEMENT

Jim McCoy, Director
Curtis Elswick, Contracts and Business Manager

AUDITORS

John Rudd – Director
Mel Bowles – Associate Director
Brian Quam – Auditor-in-Charge
Sharad Gupta – Staff Auditor
Linda Srygley – Senior IT Auditor

cc: Auditor of Public Accounts
Zack Adams
Bob Broyden
Bill Elvey
James Hyatt
Kurt Krause
Ken Miller
Dwight Shelton
Charles Steger
### Environmental, Health and Safety Training

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Design &amp; Construction (CDC) management should develop a training plan for all applicable staff and maintain training records for those individuals. The training process should include communication of the university’s Health and Safety Policy (No. 1005) and information about how employees should report hazards, accidents and injuries (see <a href="http://www.ps.vt.edu/benefits/workers/">http://www.ps.vt.edu/benefits/workers/</a> on the Personnel Services’ web site).</td>
<td>CDC staff periodically visit university construction sites that can pose occupational and industrial hazards during the excavation and construction phases. Proper training and awareness reduces the risk for injuries and/or fatalities to staff members visiting those sites. CDC management does not maintain training records for departmental staff that periodically visit project construction sites.</td>
<td>In conjunction with the Safety Engineer for Facilities, a training plan for all applicable CDCD staff is being prepared that will incorporate the pertinent information of the university’s Health and Safety Policy. Training will be scheduled to address any training gaps. Training records will be maintained in the employee’s departmental personnel file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk Evaluation: Medium Implementation Date: October 31, 2005 (expected effective date for the training plan)</td>
</tr>
</tbody>
</table>
Workstation and Server Security

**Recommendation**
Implement additional generally accepted, industry-standard guidelines for computer configuration, security and use (see http://www.security.vt.edu), including the following:

- Stronger account settings on the Capital Design and Construction server, primarily secure password requirements in accordance with university guidelines, [www.computing.vt.edu/accounts_and_access/index.html](http://www.computing.vt.edu/accounts_and_access/index.html)
- More stringent server security options and a login announcement that references the University Acceptable Use Policy
- Separate accounts with limited privileges for end-users
- A secure server location with restricted access and effective lockout procedures
- A hard copy log of changes made to the server
- Unused ports closed to prevent unauthorized access
- Contractor notification and signed acceptance of the Virginia Tech Acceptable Use Guidelines
- Secure methods of transferring files

**Benefits/Basis**
Implementation of additional security will provide assurance that the data collected on workstations and servers is protected from unauthorized access and maintains a high degree of integrity.

Audit's review of one server and eight workstations revealed relative weaknesses in both security settings and physical security, specifically:

- **Account Policy Settings** included relatively short account lockout durations and minimal requirements for password length, complexity, expiration and re-use.
- **Server “Security Options”** allowed 600 minutes idle time before disconnecting and auto-displayed the last user name at logon.
- **Server “User Rights Assignments”** were set to allow “everyone” to log on locally and shut down the system, and users have full administrative privileges on workstations.
- The server console and server room were not locked when the administrator was not present, and the password-protected screensaver has a 60 minute time-out.
- Configuration changes are not logged.

**Management Action Plan**
The Capital Design & Construction Department has reviewed university guidelines regarding computer configuration, security and use and has started implementing procedures that include:

- More secure password requirements consisting of lockout durations of 30 minutes for the server and 15 minutes for individual machines and more stringent requirements for password length, complexity, expiration and re-use. Password re-use has been set at 1-day.
- Server “Security Options” have been updated to allow only 15 min. of idle time.
- A login in announcement has been added that references the University Acceptable Use Policy. Contractors with network access will be notified regarding Acceptable Use Guidelines and are to sign an agreement to abide the those terms and conditions.
- Server “User Rights Assignments” have been updated to reflect “power user” status in lieu of “administrator” for office personnel (except Computer Systems Manager and Project Systems Manager who are “administrators”). Only administrators can now log in to the
• Unused ports were open and vulnerable.
• Machine unsecured file transfer protocol (FTP) is enabled on the server.

Password-protected screensavers on individual machines now have a timeout of 30 min. in lieu of 60 min. The server console will be locked via a password-protected screensaver when the administrator leaves the console for more than 5 minutes. The server room will be locked when the administrator and/or authorized occupants leave the room.

A log of configuration changes is being developed. Once prepared, all changes will be noted in the log when incurred.

Known unused ports have been disabled and unused ports are further blocked by a firewall.

FTP has been disabled.

**Risk Evaluation: High**

**Implementation Date: June 15, 2005**
## Disaster Recovery and Contingency Planning

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform a risk analysis to determine and document which information resources are critical to efficient departmental function. Develop and adopt an emergency response/disaster recovery plan that documents what measures will be taken now, or in the event of an emergency, to return those resources to service or to replace critical equipment and information. Store the document in a secure location for reference as needed and update it as needed or on an annual basis.</td>
<td>Identification of critical departmental resources and preliminary planning for the repair or replacement of those resources will help the department resume essential business processes in the event that an emergency or disaster occurs. Capital Design and Construction has not developed, tested, or adopted a disaster recovery/business contingency plan.</td>
<td>Capital Design &amp; Construction will be added to the existing Virginia Tech Facilities Disaster Recovery and Contingency Plan, which is updated annually.</td>
</tr>
</tbody>
</table>

Guidance can be found at [http://security.vt.edu/playitsafe](http://security.vt.edu/playitsafe).

Risk Evaluation: Medium
Implementation Date: June 15, 2005
## Software Maintenance

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital Design and Construction should seek to modify their contract with its software vendor to include provisions that would make the source code available to the university should the vendor become insolvent or otherwise could no longer support the software. System modifications and enhancements received from the vendor should be thoroughly tested before applying them to the production database.</td>
<td>Securing the source code for critical software or having it placed in trust will enable Capital Design and Construction to continue business operations and make needed modifications to the system should the vendor become insolvent. Testing system modifications for Expedition/Primavera on a test server before installing to the production database could prevent potential damage or corruption of production data.</td>
<td>Management has obtained the Primavera Expedition source code. Terms and conditions of obtaining the code were reviewed and approved of by Virginia Tech’s Office of the General Counsel. A workstation has been established to test new versions of Primavera Expedition (database server &amp; web server) prior to installing on the department's main server or individual machines.</td>
</tr>
</tbody>
</table>

Capital Design and Construction does not currently have access to the source code for Expedition/Primavera software, and updates are applied to the main production database without prior testing.

### Risk Evaluation: Medium

### Implementation Date: April 1, 2005
# Web Site

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
</table>
| Develop and implement written procedures for the administration, maintenance, testing, and security of the departmental web site to include the following:  
  - Clearly defined objectives  
  - Procedures for changes to site content and code, and subsequent testing  
  - Guidelines for granting access to secure sites and an approval process | Clearly defined objectives and procedures for the departmental web site will help ensure that information provided internally and externally is effective, up-to-date, and accurate. Enhanced documentation for the website would aid in keeping the web site functional in the event of extended absence or turnover of the site administrator.  
  - There are currently no written objectives or procedures for the departmental website. | The department’s website security plan is being modified to include the department’s website objectives and procedures. This will allow management access to written procedures in case of emergency or personnel turnover. |

**Risk Evaluation:** Medium  
**Implementation Date:** June 15, 2005
TO: Finance and Audit Committee of the Board of Visitors

FROM: John C. Rudd, Director

DATE: May 24, 2005

SUBJECT: Final Report – Dining Services

Internal Audit has completed a review of Dining Services functions in conformity with the fiscal year 2005 audit plan. The objective of this review was to contribute to the improvement of risk management and the control systems within Dining Services by identifying and evaluating the area’s exposures to business risks and the controls designed by management to reduce those risks.

BACKGROUND

Dining Services functions as a separate auxiliary enterprise within the Office of Student Programs. Dining Services sales revenue was approximately $27 million for fiscal year 2004 and employs approximately 800 classified, wage, and student employees. Dining Services, a large and complex organization, has won many national awards and is recognized as a leader in college and university food service. Dining Services operates twelve dining centers on-campus that include: two traditional board operations, a food court featuring twelve specialty venues, a marketplace café, a gourmet coffee shop, five national brand venues, and two express locations. All of these locations are supported by the Southgate Food Processing Facility. Approximately 4.3 million meals were served annually during fiscal year 2004 to students, university employees and campus visitors. Dining Services offers a number of meal plans and flexible spending options to both on-campus and off-campus students. In order to ensure that the dining programs and services meet the needs of the campus community, Dining Services provides nutritional counseling, and actively seeks customer input.

Additionally, catering services are offered to university and university-affiliated organizations.

RISK EXPOSURE

Internal Audit periodically performs a detailed risk analysis of all of the university’s auditable entities using factors such as the amount of cash inflows, operating expenditures, grant activities, level of external regulation, etc. The goal of the process is to prioritize those entities within the university that should receive audit attention. Dining Services was determined to be a high risk entity due to health & safety considerations, the volume of transactions processed, and the high volume of cash inflows.

SCOPE

The scope of this audit included the following functions: Dining Units and Catering services revenues and expenditures, food safety and hygiene, network security, disaster recovery and contingency planning. The review covered the period of July 1, 2003 to December 31, 2004.
OVERALL ASSESSMENT
Our review indicates that management has designed and implemented controls that are often effective at reducing the department’s exposure to many of the business risks it faces, but improvements are recommended to achieve a fully effective system of internal controls. Audit recommendations were issued to management where opportunities for further improvements were noted. See the attached appendices for our recommendations and management’s action plans.

MANAGEMENT:
Dr. Edward F D Spencer, Associate Vice President for Student Affairs
Rick Johnson, Director of Housing & Dining Services
Vera Kidd, Associate Director for Planning & Business Services
Robert Coffey, Senior Associate Director, Dining Services
Ted Faulkner, Associate Director, Dining Services
Kimberle Badinelli, Associate Director, Public Relations & Information Technology
Chris Moore, Business Manager Housing & Dining Services

AUDITORS:
John C. Rudd, Director
Mel Bowles, Associate Director
Divya Amin, Auditor-in-Charge
Paul Toffenetti, IT Manager
Linda Srygley, Senior IT Auditor
Sharad Gupta, Staff Auditor
Michelle Zorn, Staff Auditor

pc: Auditor of Public Accounts
    Zack Adams
    Kimberle Badinelli
    Bob Broyden
    Robert Coffey
    Landrum Cross
    Ted Faulkner
    James A. Hyatt
    Rick Johnson
    Vera Kidd
    Mark McNamee
    Ken Miller
    Chris Moore
    Dwight Shelton
    Edward F D Spencer
    Charles W. Steger
## Associate Training

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a monitoring mechanism to document and ensure that all Dining Services employees receive the appropriate training for their role as outlined in departmental policies.</td>
<td>Consistent and thorough documentation of training provided to employees would provide management with a better tool for ensuring that all employees receive the appropriate training.</td>
<td>Dining Services explored using the Banner HRIS system five years ago to implement a method of recording employee training data. Due to competing priorities for Banner projects, the Banner system has not been made available to use for this purpose, therefore, we will develop or purchase a tracking database in order to accomplish this. Food Safety &amp; Hygiene, Cashier, and bartender training will be incorporated into that database.</td>
</tr>
</tbody>
</table>

During Internal Audit’s review, the following was noted:

1. Cash Register training documentation was not adequately maintained for the following Dining units:

**Au Bon Pain** - A training log was maintained for associates hired when the dining unit was initially opened, however the training documentation for subsequent hires was not maintained.

**Sbarro, Dietrick, Owens Food Court** – Training documentation was not available for the audit period.

2. It was not evident that Food Safety & Hygiene training was provided to two of thirty employees tested.

3. Catering Services maintains a listing of trained bartenders; however, no class rosters or other documentation of such training is maintained.

### Risk Evaluation: Medium

### Implementation Date: August 31, 2005
## Fiscal Responsibility

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>A manager should review and approve the monthly reconciliation of Dining Services’ purchases recorded in the MIP (Micro Information Product) accounting system to the university’s Banner Finance system.</td>
<td>A review and sign-off of the monthly reconciliation between Banner and MIP would assist management in monitoring whether reconciliations are completed accurately and timely, and whether exceptions are corrected in a timely fashion. It would also ensure full compliance with university policy 3100 entitled <em>Fiscal Responsibility</em>.</td>
<td>Beginning with the May 2005 reconciliation, the Associate Director of Student Programs for Planning and Business Services has delegated the task of approving monthly reconciliations between MIP and Banner to the Business Manager for Student Programs. The Associate Director and the Business Manager will catch up by reviewing and signing the unsigned monthly reconciliations, (which were completed in good order and on time each month by the Business Services Accountant who handles this duty). These expense reconciliations went unsigned after the departure of the former Business Manager, and have not until now been delegated to the Business Manager who was hired to fill that position. The signatures for the unsigned months should be completed by May 31, 2005.</td>
</tr>
</tbody>
</table>

Internal Audit’s review noted that a year to date (YTD) reconciliation is performed between MIP and Banner by account code on a monthly basis; however, the reconciliation is not reviewed or approved by management.

**Risk Evaluation:** Medium  
**Implementation Date:** May 31, 2005
### Inventory

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a formal process to investigate the differences between planned usage and actual usage for dining units. This may include determining the thresholds for investigating the deviations and maintaining the supporting documentation.</td>
<td>Development of a formal process for investigating deviations in dining units' inventory and maintaining supporting documentation would ensure accuracy of the inventory and highlight potential shrinkage/shortages. Additionally, recording a perpetual alcohol inventory would ensure accuracy of the physical inventory and highlight potential shrinkage/shortages and enhance overall control over inventory.</td>
<td>Dining Services management staff does review and investigate inventory deviations within each unit, however there is no formalized and documented process for doing so. Dining Services management staff will continue to review inventory and investigate discrepancies, however, they will also begin signing and dating the FoodPro inventory analysis report weekly to provide the formal documentation of such review.</td>
</tr>
<tr>
<td>Maintain a perpetual inventory for alcohol within Catering Services to ensure the accuracy of the physical inventory taken weekly.</td>
<td></td>
<td>The Catering Department will begin keeping a perpetual inventory combining all alcohol purchased with all alcohol used in catered events. The weekly physical inventory count will be verified against the perpetual inventory, signed, and dated by the Catering Manager. All variances will be investigated and documented.</td>
</tr>
</tbody>
</table>

During Internal Audit’s review it was noted that Dining Units take a physical inventory weekly and enter the counts in the Food Pro system; however, a perpetual inventory is not maintained for comparative analysis. The dining units rely on the deviations between “planned usage” and “actual usage” of items to identify shrinkage and determine the accuracy of Inventory on hand. However, there is no formal process in place for investigating and documenting deviations. It is not evident whether deviations were investigated and the resolutions reviewed by management.

For Catering events, a physical inventory of alcohol is taken weekly. However, a perpetual inventory is not maintained for comparative analysis.

**Risk Evaluation:** Medium  
**Implementation Date:** August 31, 2005
Virginia Tech Internal Audit
Appendix
05-529 Dining Services
Recommendations

Additionally, it was not evident if the alcohol count was reviewed and approved by management.

Office Cash

**Recommendation**

Enhance the safe counting process to ensure safe counts are witnessed consistently.

Enhance physical safeguards over the cash at Owens food court. Limit access by keeping doors locked and closed.

**Benefits/Basis**

Strengthening the safe counting process would ensure safe counts are accurate and witnessed by an associate other than the office cashier. Additionally, enhancing security measures would ensure cash is safeguarded adequately.

During Internal Audit’s review it was noted that a safe count log is maintained for safe counting on a daily basis. The log indicates the date, time, safe amount, over/short, signature of the associate counting the safe and witness signature. However, daily safe counting is not witnessed consistently.

Additionally, the process for safeguarding cash could be enhanced at Owens Food court. The Student Manager office, where the cashiers count their tills and deposits, is open at all times and access to the office is unlimited. The access to the cashier’s office is through the Student Manager office and the Dutch door (top part of the door) to the cashier’s office is open at all times.

**Management Action Plan**

It is our procedure to count the safes at least once per day under dual control (usually at the shift change when the cash office supervisor leaves for the day). Depending on the dining unit, additional counting may occur at the start and close of the business day. If additional counts are performed of the entire safe fund, that count will occur under dual control. Any other access to the change fund (e.g. replenishment of tills) should be logged on the safe count log by the authorized cash office personnel, but would not be done under dual control. We are working with the Bursar’s Office to develop procedures that take into consideration the differences in staffing, safe configurations, and cash levels in different dining units. We anticipate implementation of new, approved procedures by August 2005.

The safe funds at Owens Food Court have always been secured behind a locked and alarmed door in the cash office. The door to the student managers’ office was replaced, during the audit (March 2005) with a lockable door that features a view window. This door is now locked anytime cashiers are counting tills or preparing deposits, and access is limited to management and authorized cash office personnel. The Owens management and cash office personnel have been instructed to keep the top half of the Dutch door that leads from the student managers’ office into the cash office closed anytime the safe is opened or funds are exposed. This change was implemented in March 2005.
IT Risk Analysis and Business Operations Recovery

**Recommendations**

Perform a “Business Impact/Risk Assessment for Information Technology Assets” to identify and prioritize computer hardware and software resources that are critical to departmental function.

Develop, coordinate, publish, and test an emergency response plan for business operations recovery that describes how services will be sustained after a major computer failure or other serious events.

Guidance for these recommendations can be found at: [http://security.vt.edu/playitsafe](http://security.vt.edu/playitsafe).

**Benefits/Basis**

Identification of critical department information technology resources and planning for resumption of business operations after major disruptions will mitigate the effects of such occurrences.

Dining Services previously drafted an incomplete “Emergency Operations Disaster Recovery and Contingency Plan.”

**Management Action Plan**

Student Programs’ earlier efforts to adopt a complete “Emergency Operations Disaster Recovery and Contingency Plan” including Dining Services were temporarily suspended to allow for coordination with the university’s overall continuity of operations planning. Student Programs will seek advice and assistance from Information Technology Security and Environmental Health and Safety Services to complete, test, and adopt an integrated plan prior to June 30, 2006. Many of the more critical elements of such a plan, such as provisions for providing continuity of food service for students, have already been developed. Other critical elements will be adopted in the interim as they are developed as part of the integrated plan.

**Risk Evaluation:** Medium

**Implementation Date:** June 30, 2006
## Deposits

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure timely deposits are made for Catering services in compliance with the University's Funds Handling Guidelines.</td>
<td>Timely deposits mitigate the risk of holding funds in the office safe and ensure compliance with the University's Funds Handling Guidelines.</td>
<td>At the time the deposits were made late, the Catering office only had one employee trained to prepare deposits. The Catering Department now has a backup depositor in place to ensure that deposits are made within 24 hours of receipt in the event that the primary depositor is out of the office.</td>
</tr>
<tr>
<td>Establish a process which maintains accountability for deposit bags picked up by the courier.</td>
<td>Additionally, establishing a chain of custody when deposits are picked up provides a thorough audit trail and evidence that the deposits were handed over to the courier.</td>
<td>The Bursar's Office initiated a new procedure in April 2005 whereby our staff will initial on the police courier's log when deposits are picked up.</td>
</tr>
</tbody>
</table>

Based on Internal Audit's review, it was noted that three of 20 (15%) deposits tested totaling $2,081 were deposited 1-2 days late. Also, during our review of Dining Services, it was noted that deposit bags are picked up by a courier (Virginia Tech campus police) on a daily basis. The courier indicates on his log the date, time and number of bags picked up; however, the office cashier does not retain any acknowledgement or receipt of the number of bags handed over to the courier.

**Risk Evaluation:** Low  
**Implementation Date:** April 30, 2005
## Register Voids

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain void logs for each register in the dining units and ensure that original and corrected register receipts are attached to the log for all voids.</td>
<td>Maintaining void logs for all registers would enhance accountability of the voids. Retaining original and corrected register receipts for each void allows for management review to ensure authenticity of the voids.</td>
<td>Dining Services implemented a new Voids and Corrections procedure in the fall of 2004 in response to the revised University funds handling procedures, around the same time of the documents being reviewed in this audit. Dining Services has been implementing this procedure since that time and has been working with the staff in the units to improve documentation on the Void Logs. Management and cash office personnel were reminded of the void and corrections procedures in April 2005 including the need for clear documentation, and we believe there are sufficient controls in place now to ensure that voids are handled appropriately at both the cashier level and the management level.</td>
</tr>
</tbody>
</table>

During Internal Audit’s review of the register voids, it was noted that for Owens Food Court and Dietrick dining units, a void log was not maintained for each register for the scope period. The void receipts were stapled to the shift report. Additionally for Sbarro and Au Bon Pain dining units, the original and/or corrected receipts were not attached to the Void log for several voided transactions.

**Risk Evaluation:** Low

**Implementation Date:** April 30, 2005
**IT Software Documentation**

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>The online ordering system for the “We Care” package catering operation should be fully documented or replaced with a commercial, fully-supported system that meets departmental requirements.</td>
<td>The absence of software documentation severely limits effective troubleshooting and precludes system modification and enhancement. The ordering system for the “We Care” operation was developed in-house by a technical staff member who is no longer employed by the university. During the audit, a known defect was detected in the system which had been difficult for the current technical staff to correct given the limited documentation available.</td>
<td>The defect detected during the audit has been corrected. The rare exceptions resulting from the defect had previously been identified and corrected manually. The detailed observations provided during the audit allowed the defect to be identified and eliminated. Student Programs will explore the feasibility of commercial off-the-shelf solutions to determine whether there are alternatives for “We Care” that are fully-supported and economically feasible. Alternatively, if a reasonable commercial alternative is not identified, Student Programs will ensure that the current process is fully documented by May 31, 2006.</td>
</tr>
</tbody>
</table>

**Risk Evaluation:** Low  
**Implementation Date:** May 31, 2006
# Franchise Fees

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Benefits/Basis</th>
<th>Management Action Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish a monitoring mechanism to ensure the accuracy of franchise sales records and franchise fees calculated.</td>
<td>Additional monitoring of franchise sales and fees computations would mitigate the risk of reporting incorrect sales and paying inaccurate fees to the franchisor. During Internal Audit’s review, we noted that Dining Services own five franchises. Franchise fees are paid to the franchisor on a monthly basis. For Au Bon Pain it was noted that sales for March 2004 were understated by $14,150. As a result franchise fees submitted to the franchisor were $707 less than required by the contract. The additional fees were submitted to the franchisor during the audit.</td>
<td>During the audit period, franchise reports were prepared at the dining unit level and sent directly to the business office for processing. Effective April 2005, the Administrative and Systems Specialist will verify the calculations on franchise sales reports prior to submission to the Student Programs Business Services office for payment processing to ensure that the computed sales and corresponding royalty payment are accurate.</td>
</tr>
</tbody>
</table>

**Risk Evaluation:** Low  
**Implementation Date:** April 30, 2005