



---

# Technology Standard

---

## Virginia Community College System (VCCS) Information Technology Audit Plan

Version: 1.0

Status: *Approved: 02/21/07*

Contact: [Vice Chancellor Information Technology Services](#)

---

### PURPOSE

To establish an IT Security Audit Plan for the period July 1, 2007 – June 30, 2010. The plan also identifies and assigns appropriate responsibility to those individuals who have been designated to ensure VCCS complies with all the provisions included in the Commonwealth of Virginia Information Technology Security Audit Standard ([ITRM Standard SEC502-00](#)).

---

### AUDIT PLAN

#### General

The VCCS three year audit plan covers the period starting July 1, 2007 and ending June 30, 2010 and includes four primary audit objectives.

#### **Year One: July 1, 2007 – June 30, 2008**

There are two audit objectives included in the year one plan. The first objective is a high level review of the System Office and twenty-three college's use of the Commonwealth's Payroll and Personnel Systems. The second objective will include a review of the college local area networks.

**Audit Objective #1:** Payroll and Personnel Systems

## **Description:**

The plan will review internal operations at the System Office and a select number of the twenty-three colleges to properly assess the System compliance in accordance with the requirements of the Commonwealth of Virginia Information Technology Security Standard ([ITRM Standard SEC501-01](#)). The systems that will be reviewed are:

PMIS (Personnel Management Information System)

CIPPS (Commonwealth Integrated Personnel/Payroll System)

## **Scope of Work**

- Measure compliance with applicable requirements of the COV IT Security Policy ([ITRM SEC500-02](#)) and COV IT Security Standard ([ITRM SEC501-01](#)).
- Measure compliance with applicable VCCS Standards, Models, and Guidelines.
- Measure compliance with external applicable requirements (HIPAA for example).

## **IT Security Audit Schedule**

The VCCS Internal Audit Office in consultation with the Information Technology Services Office will identify the colleges to be included the FY08 audit plan choosing a representative sample. The goal is to complete all the associated audits on or before June 30, 2008 using a schedule that best accommodates the System Office, colleges being audited, and the Internal Audit staff.

## **Checklist of Information and Access Required for the IT Security Audit**

The System Office will provide the college with a list of information as necessary for review during the audit process and specify access to systems or data needed by the audit staff to perform the required audit.

## **Documentation of the Audit**

- The Internal Audit Office will prepare work papers and safeguard them appropriately.
- The Internal Audit Office will document the findings of the audit and issue a report to the college president.
- The college president shall prepare a corrective action plan to include
  - For concurrence...
    - Corrective action
    - Date for the corrective action
    - Who is responsible for the corrective action
  - For non-concurrence...
    - College statement of position
    - Mitigating controls in place

- Colleges acknowledgment of acceptance of risk
- The Internal Audit Office will ensure the college president completes all corrective action plans and verify their implementation.
- The VCCS CIO/Vice Chancellor of Information Technology Services (ITS) will report all audit results to VITA at least once each quarter.

## **Audit Objective #2: College Local Area Networks**

### **Description:**

This audit is intended to provide a review of the implemented security provisions at the VCCS through a selective sampling of the college campus local area networks from both an internal and external perspective. It will provide insight into the Information Security (INFOSEC) status of each location sampled as it relates to the provisions included in published VCCS network standards, guidelines, and procedures.

### **Scope of Work:**

The review will have three distinct phases:

Phase 1 Security of the College/Campus Network Infrastructure

Phase 2 Segmentation of the Local College/Campus Network

Phase 3 Assessment of the College/Campus Networks Compliance with Information Technology Policies, Standards, and Guidelines

### **IT Security Audit Schedule**

The VCCS Internal Audit Office and the Information Technology Services Office will prepare a statement of work to be used in acquiring the services of an external provider for completing this review. The ITS Office will identify the colleges to be included in the audit. The goal is to complete all the associated audits on or before June 30, 2008. The schedule will be included with the final audit program.

### **Checklist of Information and Access Required for the IT Security Audit**

The VCCS Internal Audit Office will provide each college with a checklist of information as necessary for review during the audit process and specify access to systems or data needed by the audit staff to perform the required audit.

### **Documentation of the Audit**

- Work papers will be prepared and safeguarded appropriately.
- The Internal Audit Office will document the findings of the audit and issue a report to the college president.

- The college president shall prepare a corrective action plan to include
  - For concurrence...
    - Corrective action
    - Date for the corrective action
    - Who is responsible for the corrective action
  - For non-concurrence...
    - College statement of position
    - Mitigating controls in place
    - Colleges acknowledgment of acceptance of risk
- The Information Technology Services Office will ensure the college president completes all corrective action plans and verify their implementation.
- The Vice Chancellor for Information Technology Services will report all audit results to VITA at least once each quarter.

### **Year Two: July 1, 2008 – June 30, 2009**

The second year plan includes a detailed review of the Student Information System.

#### **Audit Objective #3: Student Information System (SIS)**

##### **Description:**

The plan will review operations at the System Office and a select number of the twenty-three colleges to properly assess the System compliance in accordance with the requirements of the Commonwealth of Virginia Information Technology Security Standard ([ITRM Standard SEC501-01](#)).

##### **Scope of Work**

- Measure compliance with applicable requirements of the COV IT Security Policy ([ITRM SEC500-02](#)) and COV IT Security Standard ([ITRM SEC501-01](#)).
- Measure compliance with applicable VCCS Standards, Models, and Guidelines.
- Measure compliance with external applicable requirements (HIPAA for example).

##### **IT Security Audit Schedule**

The VCCS Internal Audit Office in consultation with the Information Technology Services Office will identify the colleges to be included the FY09 audit plan choosing a representative sample. The goal is to complete all the associated audits on or before June 30, 2009 using a schedule that best accommodates the System Office, colleges being audited, and the Internal Audit staff.

##### **Checklist of Information and Access Required for the IT Security Audit**

The System Office will provide the college with a list of information as necessary for review during the audit process and specify access to systems or data needed by the audit staff to perform the required audit.

### **Documentation of the Audit**

- The Internal Audit Office will prepare work papers and safeguard them appropriately.
- The Internal Audit Office will document the findings of the audit and issue a report to the college president.
- The college president shall prepare a corrective action plan to include
  - For concurrence...
    - Corrective action
    - Date for the corrective action
    - Who is responsible for the corrective action
  - For non-concurrence...
    - College statement of position
    - Mitigating controls in place
    - Colleges acknowledgment of acceptance of risk
- The Internal Audit Office will ensure the college president completes all corrective action plans and verify their implementation.
- The VCCS CIO/Vice Chancellor of Information Technology Services (ITS) will report all audit results to VITA at least once each quarter.

### **Year Three: July 1, 2009 – June 30, 2010**

The FY10 plan will include a review of the Administrative Information System (AIS).

#### **Audit Objective #4: Administrative Information System (AIS)**

##### **Description:**

The plan will review internal operations at the System Office and a select number of the twenty-three colleges to properly assess the System compliance in accordance with the requirements of the Commonwealth of Virginia Information Technology Security Standard ([ITRM Standard SEC501-01](#)).

##### **Scope of Work**

- Measure compliance with applicable requirements of the COV IT Security Policy ([ITRM SEC500-02](#)) and COV IT Security Standard ([ITRM SEC501-01](#)).
- Measure compliance with applicable VCCS Standards, Models, and Guidelines.
- Measure compliance with external applicable requirements (HIPAA for example).

##### **IT Security Audit Schedule**

The VCCS Internal Audit Office in consultation with the Information Technology Services Office will identify the colleges to be included the FY10 audit plan choosing a representative sample. The goal is to complete all the associated audits on or before June 30, 2010 using a schedule that best accommodates the System Office, colleges being audited, and the Internal Audit staff.

### **Checklist of Information and Access Required for the IT Security Audit**

The System Office will provide the college with a list of information as necessary for review during the audit process and specify access to systems or data needed by the audit staff to perform the required audit.

### **Documentation of the Audit**

- The Internal Audit Office will prepare work papers and safeguard them appropriately.
  - The Internal Audit Office will document the findings of the audit and issue a report to the college president.
  - The college president shall prepare a corrective action plan to include
    - For concurrence...
      - Corrective action
      - Date for the corrective action
      - Who is responsible for the corrective action
    - For non-concurrence...
      - College statement of position
      - Mitigating controls in place
      - Colleges acknowledgment of acceptance of risk
  - The Internal Audit Office will ensure the college president completes all corrective action plans and verify their implementation.
  - The VCCS CIO/Vice Chancellor of Information Technology Services (ITS) will report all audit results to VITA at least once each quarter.
- 

[Return to Information Security Program](#)