

---

# Off-Line

*The SC Midlands Chapter of the Information Systems Audit & Control Association*

---

CHAPTER 54

AUGUST 2007

## September Seminars:

### Computer Security:

How to Audit Security on Any Type of Computer

How to Audit MVS, RACF, Top Secret, USS, and TCP/IP



Once considered mostly relics of a computing era gone by, the mainframe remains with us. In fact, mainframes are experiencing something of a resurgence today. Their inherent reliability and stability well equip them for hosting large virtual environments or serving as the information hub in a service oriented architecture (SOA).

IBM recently announced a five year, \$100 million initiative to simplify mainframe operations including graphical user interfaces and more automated routines. According to Clabby Analytics, an industry based research group, the initiative “is intended to make mainframe technology appeal to the next generation of Windows-born-and-trained managers and administrators.” In addition, IBM reported that revenues from mainframes grew 12% in the first quarter of 2007. It appears that mainframes are not yet relegated to “the sunny slopes of days gone by”.

We are pleased to present two computer security seminars including a three-day course specifically focused on mainframe security. Both seminars feature the nationally recognized speaker and consultant in computer security and training, Stu Henderson

## Two Training Opportunities

**How to Audit Security on Any Type of Computer** is a half-day seminar that gives auditors a model for evaluating security on any type of computer. Presented in partnership with The Palmetto Chapter of the IIA, this seminar is suitable for auditors of all types: IT, financial, and operational. Attendees will learn in simple terms, illustrated with Stu Henderson's internationally famous artwork, how computer security works and how to audit it on any type of computer. The seminar includes the following:

### Introduction

- The basic model
- Why the two parts of the model are both essential
- The Kindergarten Scenario -- What is an Operating System

### The First Part: the Trusted Computing Base

- How the Hardware Controls Work
- How the Operating System Uses Them
- The Concept of "Backdoors"
- How This Works on Windows, on UNIX, on the Mainframe
- How to Audit This All, Regardless of Computer Type

### The Second Part: the Q1Q2 Model

- Question 1 and How It Gets Answered
- Question 2 and How It Gets Answered
- How This Works on Windows, on UNIX, on the Mainframe
- How to Audit All This, Regardless of Computer Type

**How to Audit MVS, RACF, Top Secret, USS, TCP/IP** is a three-day seminar building on the concepts outlined above and specifically focused on mainframe computer security systems. The seminar will show auditors and security professionals how to audit these critical software components of z/OS. The extensive course workbook is also a valuable reference guide. For each of the components, students will learn how the software works, including:

### Introduction

- Keywords and Concepts
- Audit Rules
- What the Software Components Are and How They Relate

### MVS

- How Its Security Works
- How to Audit Its Security

### RACF

- How Its Security Works
- How to Audit Its Security

### Top Secret

- How Its Security Works
- How to Audit Its Security

### USS (UNIX under MVS)

- How Its Security Works
- How to Audit Its Security

### TCIP/IP

- How Its Security Works
- How to Audit Its Security

## About the Speaker

Stu Henderson ([www.stuhenderson.com](http://www.stuhenderson.com)) is a nationally recognized speaker and experienced consultant who specializes in computer security and training. He has helped hundreds of organizations make better use of security software such as RACF, ACF2, and TopSecret. He has conducted MVS security reviews for numerous commercial and government organizations. He communicates effectively with all levels of staff, from computer operator to executive management. He has over twenty-five years of hands-on experience as a system programmer, Data Security Officer, and consultant, culminating in his founding his own consulting organization, the Henderson Group.

Stu's experience includes nine years with AT&T, where he was responsible for both MVS and VM technical support and maintenance. While there, he initiated the computer measurement function for both MVS and VM, using software monitors and SMF data for chargeback, capacity planning, and system tuning. His extensive hands-on experience there, with both hardware and software for mainframes and networks, provided the technical basis for his subsequent computer security practice.

At a major brokerage firm he created the computer security function, including complete implementation of RACF security software, development of security policy and procedures, and development of techniques for analysis of SMF data to monitor violations and out-of-norm usage. In two years his computer security work earned him promotions to Assistant Vice President and Vice President.

Working as a consultant for firms such as Ernst & Ernst (now Ernst & Young) and Coopers & Lybrand, he developed systematic approaches to evaluating computer security. He taught these approaches to other consultants and auditors, and used them successfully in security reviews at client data centers. At Coopers & Lybrand, where he was director of Computer Security Services for the Mid-Atlantic Region, he created the C&L Computer Security seminar series. This included security seminars addressing: MVS, TopSecret, ACF2, RACF, VTAM, and DB2. Stu developed and taught most of the seminars himself.

Since 1990, he has directed his own firm, the Henderson Group, which provides computer security consulting and training in a variety of technical areas, including: MVS, OS/390, z/OS and Windows/NT/2000 security reviews, implementation assistance to users of RACF, ACF2, and TopSecret, and assistance to audit departments conducting MVS and Windows security audits. He founded the New York RACF Users Group and edits the RACF newsletter with a circulation of over 2500. Stu also supports Computer Security Tech Support Hotline for MVS Data Security Officers and IT Auditors.

## TWO LOCATIONS

The half-day seminar will be held at Seawell's on Rosewood Drive. This seminar also serves as the opening meeting for the 2007-2008 Palmetto IIA Chapter year. The seminar will begin at 11:00, include lunch, and end at 4:00.

The three-day seminar will be held at Blue Cross Blue Shield offices on Percival Road. This course will build upon concepts and models presented in the opening half-day seminar. It is highly recommended that mainframe students attend both seminars. The seminar will begin at 8:00 each morning ending by 5:00. Directions to the Blue Cross offices:

**From Camden, SC** take I-20W to exit #80/Clemson Road. Turn left onto Clemson Road. Turn right onto Percival Road and stay right turning into the parking lot of the office.

**From Charlotte, NC**, take I-277 S to exit #1B/Columbia onto I-77S. Go approximately 85 miles. Take exit #16A/Florence onto I-20E. Take exit #80/Clemson Road. Turn right onto Clemson Road. Turn right onto Percival Road and stay right turning into the parking lot of the office.

**From the Columbia Metropolitan Airport**, Start on Airport Blvd going toward Aviation Way, Turn right on Lexington Dr. Turn right on John N Hardee Expressway, Turn left on SC-302, Take ramp onto I-26 E, Take left exit #116/Charlotte onto I-77 N for approximately 15 miles, Take exit #16/Augusta/ Florence onto I-20 E toward Florence. Exit onto Clemson Road (Exit #80). Turn right onto Clemson Road. Turn right onto Percival Road and stay right turning into the parking lot of the office.

**From the Irmo/Lexington area**, take I-26 E. Exit onto I-20 E toward Florence and travel approximately 15 miles. Exit onto Clemson Road (Exit #80). Turn right onto Clemson Road. Turn right onto Percival Road and stay right turning into the parking lot of the office.

**From Columbia**, take I-20 toward Florence. Exit onto Clemson Road (Exit #80). Turn right onto Clemson Road. Turn right onto Percival Road and stay right turning into the parking lot of the facility.

**Note:** You may park in any space outlined in white. Proceed to the Lobby at the center front of the building and obtain a Visitor Pass. This will require a photo id. Blue Cross staff will meet you in the lobby and direct you to the classroom. Coffee, juices and a light breakfast will be served in the morning, lunch and a light snack in the afternoon. Contact Sue Rusher at 803-264-7631 with concerns.

## REGISTRATION

ISACA and IIA are pleased to offer affordable, local, high quality training events to meet the needs of our members. These seminars will require registration and pre-payment as detailed on the following registration form:

## REGISTRATION FORM

### HALF-DAY SEMINAR: HOW TO AUDIT SECURITY ON ANY TYPE OF COMPUTER

<b>LOCATION:</b> Seawells 1125 Rosewood Dr Columbia, SC 803-771-7385	<b>DATE:</b> Monday, September 24, 2007 11:00 AM – 4:00 PM (includes lunch) 4 CPE
--	--

### THREE-DAY SEMINAR: HOW TO AUDIT z/OS WITH MVS, RACF, TOP SECRET, USS AND TCP/IP

<b>LOCATION:</b> Blue Cross Blue Shield 4101 Percival Road Columbia, SC 29229	<b>DATE:</b> Tuesday, September 25 – Thursday, September 27, 2007 8:00 AM – 5:00 PM (includes continental breakfast, lunch) 24 CPE
--	---

### REGISTRATION

Registration and pre-payment is required for the seminars and must be received by Friday, September 7, 2007. The Palmetto Chapter of the IIA will be responsible for receiving and processing payments for both seminars. Please complete this registration form and submit payment to:

The Palmetto Chapter of the IIA  
 ATTN: Mike Otero  
 PO Box 2547  
 Columbia, SC 29202-2547

- I will attend **only** the half-day seminar . . . . . \$ 100.00
- I will attend **only** the three-day seminar . . . . . \$ 450.00
- I will attend **both** the half-day and three-day seminar . . . . . \$ 500.00

TOTAL AMOUNT ENCLOSED: \_\_\_\_\_

NAME: \_\_\_\_\_

COMPANY: \_\_\_\_\_

E-MAIL: \_\_\_\_\_ PHONE: \_\_\_\_\_