Theodore W. Grolimund
Certified Information Systems Auditor, Certified Information Systems Security Professional

P.O. Box 6561 Alexandria, VA 22306-6561
703-660-6662 theodoreg@aol.com

Independent Auditor Report
On Applying Agreed Upon Procedures
To
SEC's Year 2000 Internal Efforts: Certification & Contingency Planning

Executive Summary

The Securities and Exchange Commission (SEC), Office of Inspector General (OIG) engaged the services of an independent certified information systems auditor (CIS auditor) to assess the progress of the Commission in making its automated systems year 2000 (Y2K) compliant. Under the statement of work, the CIS auditor was not responsible for testing Commission systems to determine whether they were compliant.

This audit is a continuation of audit work begun by the OIG in fiscal year 1998. The OIG has issued several progress reports detailing the progress to date and making recommendations to enhance the Commission's efforts (*i.e.*, Audit Memorandum No. 8, EDGAR Year 2000 Compliance, May 18, 1998; Audit No. 285, Y2K Status Report, issued August 24, 1998; Audit No. 293, Y2K Status Report, issued January 25, 1999; Audit No. 297, EDGAR Y2K Status, issued March 19, 1999).

Under the audit program prepared by the CIS auditor, the auditor performed agreed-upon procedures on SEC's Y2K certification process for internal mission critical systems and on the SEC's internal contingency planning efforts for the Year 2000 (Y2K). These agreed-upon procedures were performed solely to assist the OIG in evaluating internal certification processes and contingency planning efforts within the Commission.

This report is intended for use of the SEC OIG and management; however, this report is a matter of public record and its distribution is not limited. No opinion is offered on the sufficiency of evidence to support any SEC system as Year 2000 compliant, nor is any opinion being given to certify any SEC system as Year 2000 compliant. Additionally, the audit scope intentionally does not cover any Y2K aspects of the securities industry for which the SEC has oversight authority.

Audit Results in Brief:

In regards to Y2K compliance status and contingency planning activities, we obtained a copy of a letter from an independent contractor that indicated to Chairman Levitt on September 2, 1999, the following:

- The SEC has completed the Year-2000 (Y2K) renovation and validation of the Commission's automated systems. All mission-critical systems and other operational-support systems, intended to operate in the Y2K time frame, are now fully Y2K compliant in accordance with General Accounting Office (GAO) guidelines,
- Y2K complaint systems have either been placed into full production or are on schedule to complete the transition to full production,
- An initial baseline set of contingency plans related to SEC mission-critical systems has been completed, and
- Validation of these contingency plans is anticipated during November 1999.

At the time of the audit, the SEC's Year 2000 Contingency Plan and the Office of Information Technology's (OIT) contingency plans were still being refined. A readiness test of the EDGAR backup site was successfully performed on August 21, 1999. The Commission plans additional testing. Good business practices indicate that contingency plans should be tested. Untested plans can lead to a false sense of security.

As originally conceived in SEC's Year 2000 Program Management Plan, certification of systems as year 2000 compliant was intended to take place after Y2K testing and remediation but before putting systems into operation (*i.e.*, production status). However, however, the Plan was superseded by new direction from the Chairman in January 1999.

According to OIT, the Chairman mandated copious, widespread Y2K testing, and remediation of all new systems, infrastructure, and external services by August 31, 1999. Documentation (including final certification sign-off and extensive supporting documentation) would occur as soon as practicable thereafter. OIT noted that users were involved in testing, not just in certification of systems.

Since August 1999, the Commission has made progress in certifying its systems. The judgmental sample of 53 mission critical systems used for this audit indicated that on August 28, 1999, only 7 systems were certified. As of October 22, 1999, 23 systems were certified, with 20 systems pending certification.

Our findings and recommendations are listed in the Audit Results section of the report. For the short term (by the millennium date), the report recommends completing the certification process, and completing and testing contingency plans. For the long term, OIT should build on the accomplishments of the Y2K project, by implementing policies and procedures for inventorying and certifying systems, change control, ownership of systems, and contingency plans.

A draft of the report was provided for comment to OIT and the Office of the Executive Director (OED) on November 2, 1999. The report was appropriately modified based on the informal comments received. In its comments, OIT described numerous positive aspects to the SEC's Y2K compliance program:

- OIT kept senior Commission officials and the Chairman fully briefed on program status on a regular basis,
- regular communications were held between the Y2K team and the program offices on their specific systems,
- OIT appropriately expanded the role of its independent IV&V consultant to address the expanded scope of testing directed by the Chairman,
- OIT met the goal set by the Chairman,
- the SEC followed all GAO guidelines during the Y2K process, and
- the SEC Y2K program included PC applications and all infrastructure.

SCOPE AND METHODOLOGY

The Securities and Exchange Commission (SEC), Office of Inspector General (OIG) engaged the services of an independent certified information systems auditor to assess the progress of the Commission in making its automated systems year 2000 compliant. The auditor performed agreed-upon procedures on the SEC's certification process for internal mission critical systems and on the internal contingency planning efforts for the year 2000. These agreed-upon procedures were performed solely to assist the OIG in evaluating internal certification processes and contingency planning efforts within the Commission.
No representation regarding the sufficiency of these agreed upon procedures is being made.

The agreed-upon procedures were to:

- Evaluate the certification process using a judgmental sample of internal mission critical applications,
- Perform limited inquiries on contingency planning for internal information technology (IT) systems maintained by the Office of Information Technology (OIT), and
- Perform limited inquiries to the SEC's Y2K Project Coordinator within the Office of the Executive Director (OED) on business contingency planning activities in the event of internal IT system interruptions.

Procedures included interviewing key OIT and OED personnel, reviewing relevant policies and documentation, and reviewing prior OIG reports and recommendations that may be applicable to this audit. To assist our evaluation of the certification process a judgment sample was used.

This judgmental sample represents the 53 internal mission critical systems (applications) reported in SEC's June 1998 report to the Congress (Second Report on the Readiness of the United States Securities Industry and Public Companies To Meet the Information Processing Challenges of the Year 2000). In addition, GAO's publications entitled Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21) and Year 2000

Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19) were obtained to identify applicable best practice criteria.

No opinion is being given on the sufficiency of evidence to support any SEC system as Year 2000 compliant, nor is any opinion being given to certify any SEC system as Year 2000 compliant. In addition, the audit scope intentionally excludes any Y2K aspects of the securities industry for which the SEC has oversight authority.

This engagement was performed in accordance with the General Accounting Office's *Government Auditing Standards* and standards established by the Information Systems Audit Control Association (ISACA). The fieldwork was performed from September 2, 1999 through October 28, 1999. Following SEC OIG practices, a discussion draft of the report was provided for comment to OIT and OED on November 2, 1999. A copy was also provided to the OIG.

This report is intended for the use of the SEC OIG and management; however, the report is a matter of public record and its distribution is not limited.

Background

This audit is a continuation of prior audit work done by the Office of Inspector General. The OIG has already issued the following reports on the Year 2000 project: Audit Memorandum No. 8 (May 18, 1998); Year 2000 Compliance (Audit Report No. 285 - August 24, 1998); Year 2000 Status Report (Audit Report No. 293 - January 25, 1999); and EDGAR Y2K Status (Audit No. 297 - March 19, 1999). An independent CPA firm under contract with the OIG also performed an audit of non-information technology Y2K compliance, covering embedded systems such as elevators, building and fire security systems (Audit no. 291-Year 2000 Non-Information Technology, issued August 9, 1999). This report is expected to be the last formal OIG report on Y2K.

The Commission's Y2K compliance effort includes literally thousands of hardware and software items. The table below provides a brief summary of items involved. EDGAR, the Commission's premier and most critical system, is included as one of the 187 software applications.

Summary of Y2K Compliance Efforts (1)	
Infrastructure:	2,915 Windows or OS/2 workstations, 1067 laptops, 145 servers, 152 network components retired
Software:	187 applications 593 commercial or governmental products including 190 mainframe software products
External:	69 data file exchanges with 24 partners 72 commercial services (e.g. Bloomberg)

Note (1): Source: Data obtained from the SEC's Office of Information Technology.

As implemented at the SEC, Y2K compliance and Y2K certification are not synonymous. Y2K compliance indicates that Y2K testing and applicable remediation occurred. Y2K certification indicates that the system owner has accepted the system and certified it as Y2K compliant before placing it in operation.

The Year 2000 Program Management Plan, dated September 11, 1998, identifies the policies governing Y2K compliance and certification. For example, section 3.2.1 of the Plan states that "all application software, system software, system hardware, third-party software and third-party hardware used in the SEC's systems operations, development, maintenance, support and testing activities must adhere to the Y2K compliance definition."

The Y2K compliance definition is documented in SEC's Y2K Compliance Standards, Appendix C of the Program Management Plan. Section 3.4.8 of the Plan states that "the application owner will complete the certification and will sign, along with the certifying official that the application is Y2K compliant and ready for implementation into the production environment."

As originally intended by the Plan, certification was intended to take place after Y2K testing but before putting a system into operation. The certification packet includes certification recommendations, and Y2K test exceptions and discrepancies. The system is certified in writing by the system owner, the Y2K Project Director in the OED, and Y2K Director in OIT.

Audit Results

(Findings & Recommendations)

I. Certification Process

Originally, certification was planned to be part of the Y2K compliance process, as indicated in the SEC's Year 2000 Program Management Plan. OIT management indicated that this plan was superseded in January 1999. At that time, the Chairman directed widespread testing and remediation of all Commission systems by August 31, 1999 , with the understanding that documentation, including certification, would occur as soon as practicable after systems were made compliant. The Commission notified the Office of Management and Budget of this internal deadline.

An independent contractor performing IV&V (independent verification and validation) activities sent a letter to the Chairman on September 2, 1999, which indicated that

- as of August 31, 1999, the Commission had completed Y2K renovation and validation of the Commission's automated systems,
- all mission-critical and other operation support systems, intended to operate in the year 2000, were now fully Y2K compliant, in accordance with GAO guidelines, and

- Y2K compliant systems had either been placed into full production or were on schedule to complete the transition to full production.

To help ensure that systems remained complaint, the SEC's Executive Director directed that no major changes be made to software applications, operational environment, telecommunications, and infrastructure until March 2000.

To evaluate the certification process over SEC's internal systems, a judgmental sample of 53 mission critical applications was used. These systems were reported in the SEC's June 1998 report to the Congress on the Y2K readiness of the United States securities industry and public companies.

As of August 28, 1999, OIT indicated that seven systems in our judgmental sample had been formally certified as Y2K compliant. As of October 22, 1999, the number of certified systems had increased to 23. See the table below.

Certification Status of 53 Mission Critical Applications (As Of October 22, 1999)	
Certified	23
Pending Certification	20
Retired without replacement	9
Dropped	1

Source: Prepared by independent auditor, Office of Inspector General

OIT indicated that it is preparing extensive documentation for each certification package, which in part explains why certification is not yet complete. It intends to complete certification of the remaining systems as rapidly as possible, while maintaining documentation quality.

Recommendation:

A. In consultation with system owners and the OED, OIT should certify all systems by the millennial date (January 1, 2000).

Business Continuity and Contingency Planning Efforts

Based on the auditor's limited inquiries to the Y2K Project Director and OIT management, the SEC is progressing in developing its internal contingency plans. No opinion is expressed on the sufficiency of these plans.

An independent contractor, in a letter dated September 2, 1999, indicated that an initial baseline set of contingency plans for mission critical systems had been completed. The contractor stated that validation of these plans is anticipated during November 1999.

The auditor obtained a report on a readiness test of the EDGAR back-up site performed August 21, 1999. The EDGAR contractor concluded, based on the test, that the EDGAR back-up site was properly configured and provides a back-up capability for the production system.

We understand that the Commission intends to perform additional testing. Good business practices indicate that continuity and contingency plans should be tested. Untested plans can lead to a false sense of security.

Recommendation:

B. OIT should complete and test its Y2K contingency plans by January 1, 2000.

Long Term Issues

While the Y2K project has involved significant resources and much hard work, it has also brought benefits to the SEC's management of information resources. In consultation with user offices and the OED, OIT has developed an inventory and certified SEC automated systems, determined system ownership, implemented change control policies, and developed business contingency plans, among other steps.

These accomplishments need to be maintained in the long term by instituting appropriate policies and procedures.

Recommendation:

C. In consultation with user offices and the OED, OIT should implement policies and procedures covering the issues mentioned above.