Theodore W. Grolimund
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CISSP)

P.O. Box 6561 Alexandria, VA 22306-6561
703-660-6092 theodoreg@aol.com

Year 2000 Internal Efforts: Certification & Contingency Planning Status

Executive Summary

.
The Securities and Exchange Commission (SEC), Office of Inspector General (OIG) engaged the services of a certified information systems (CIS) auditor to perform agreed-upon procedures on SEC's certification process for internal mission critical systems and for reviewing 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.

The agreed-upon procedures were to:

- Evaluate the certification processes of internal mission critical applications,
- Perform limited inquiries on contingency planning activities over internal information technology (IT) systems maintained by the Office of Information Technology (OIT), and
- Perform limited inquiries to 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.

The audit scope intentionally does not cover any Y2K aspects of the securities industry for which the SEC has oversight authority. In addition, 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.

Results In Brief:

- The Commission is making progress in certifying its systems.
- The concepts behind certification support good management practices.
- In regards to Y2K compliance status and contingency planning activities, we obtained a copy of a letter from an independent contractor that indicated to the Chairman on September 2, 1999, the following:
  ⇒ *As of August 31st, 1999, the SEC has successfully completed the Year-2000 (Y2K) renovation and validation of the Commission's automated information systems. All mission-critical systems and other operational-support systems, intended to operate in the Y2K timeframe, are now fully Y2K compliant in accordance with General Accounting Office (GAO) guidelines,*

- ⇒ *Y2K compliant 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*
- ⇒ *During November 1999, these contingency plans will be validated and promulgated across the Commission.*

- A readiness test of the EDGAR backup site was performed on August 21, 1999. The EDGAR contractor concluded that the EDGAR back-up site was properly configured and provides a back-up capability for the production system.
- During the audit, SEC's Year 2000 Contingency Plan[1] and OIT's contingency plans were still being refined. Additional testing by the Commission is planned.

Recommendations in Brief:

- The Executive Director and the Chief Information Officer should ensure that business and information technology contingency plans are tested (*i.e. validated*) as planned prior to the Year 2000.

For the long term, the Commission should maintain and build upon the accomplishments of the Y2K effort to improve overall management of SEC's information resources. The lessons learned from the Y2K effort should be used to guide the development of policies and procedures to support best practices.

- The Executive Director and Chief Information Officer (CIO) should ensure that appropriate policies and procedures are implemented to maintain and test business and information technology contingency plans,
- Jointly, the CIO and Executive Director should issue Commission-wide policies and procedures to identify and assign system and data ownership roles and responsibilities,
- The CIO should implement policies and procedures to authorize and revalidate system processing,
- The CIO should continue sponsoring the certification process of the remaining uncertified systems, and
- The CIO should implement policies and procedures to improve system life cycle management (*i.e. change-controls, configuration management, quality assurance*).

Observations and recommendations are listed in the Audit Results section of the report. A draft of the report was provided for comment to OIT, the Office of the Executive Director (OED) and OIG on November 2, 1999. Various comments were received and the report was modified as appropriate.

Scope & Methodology

[1] SEC's Year 2000 Contingency Plan is sponsored within the Office of the Executive Director.

The Securities and Exchange Commission (SEC), Office of Inspector General (OIG) engaged the services of a certified information systems auditor. The CIS auditor performed agreed-upon procedures on SEC's certification process for internal mission critical systems and reviewing 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. No representation regarding the sufficiency of these agreed upon procedures is being made.

The agreed-upon procedures were to:

- Evaluate the certification processes using a judgmental sample of internal mission critical applications,
- Perform limited inquiries on contingency planning activities over internal information technology (IT) systems maintained by the Office of Information Technology (OIT), and
- Perform limited inquiries to 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 the evaluation of the certification process a judgment sample was used. This judgmental sample represents the 53 internal mission critical systems reported in SEC's June 1998 report to Congress (Second Report on the Readiness of the Unites 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. Office of Management and Budget's (OMB) Circular A-130 was also used as 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 2nd, 1999, through October 28th, 1999. This report is intended solely for the information and use of the SEC OIG and management, however this report is a matter of public record and its distribution is not limited.

Background

The Office of Inspector General (OIG), United States Securities and Exchange Commission initiated a series of reports and memoranda on the Commission's efforts to reduce internal Year 2000 (Y2K) vulnerabilities. The OIG in its continuing efforts on the Year 2000 problem engaged the services of a certified information systems (CIS) auditor under Purchase Order No. PCHQ990625[2] to complete the OIG's Year 2000 audit efforts.

Previously, the OIG issued the following reports on the Year 2000 problem: 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). The OIG also contracted with an independent CPA firm to audit non-information technology areas for Y2K compliance over embedded systems such as elevators, building and fire security systems (Audit No. 291-Year 2000 Non-Information Technology, August 9, 1999).

An independent contractor performing IV&V (independent verification and validation) activities sent a letter to the Chairman which indicated in-part that:

- as of August 31st, 1999, the Commission had successfully completed Y2K renovation and validation of the Commission's automated information systems,
- all mission-critical systems and other operational-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.

As implemented at the SEC, Y2K compliance and Y2K certification are not synonymous. Y2K compliance indicates that Y2K testing and applicable remediation occurred, whereas certification indicates that the system owner has accepted the system. As originally conceived in SEC's Year 2000 Program Management Plan, certification was to be part of the Y2K compliance process indicating (see Section 3.4.8) 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." Certification was intended to take place after Y2K testing but before putting a system into production. Subsequently, the Plan was superseded (as explained below) whereby Y2K certifications of Y2K compliant systems would take place generally after the systems were in production. Consequently, Y2K compliance and Y2K certification have different connotations. An uncertified application or system does not necessarily imply that it is not Y2K compliant.

The Chief Information Officer and other senior officials within the Office of Information Technology (OIT) indicated the Year 2000 Program Management Plan was superseded due to operational demands in January 1999 when the Chairman directed widespread testing and remediation of all systems by August 31st, 1999, with the full understanding among system owners and other senior Commission officials that documentation including certification would occur as soon as practicable thereafter. The Commission's

[2] Purchase Order Number PCH0990625 issued on June 8, 1999, includes non-related Y2K work.

Y2K compliance effort included figuratively 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	
Infrastructure:	2,915 Windows or OS/2 workstations 1,067 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)

Source: Data obtained from the SEC's Office of Information Technology.

To help ensure that Commission systems remained Y2K compliant, the Executive Director issued a memo reminding Division Directors, Office Heads, Regional Directors and District Administrators that Y2K compliance must be maintained and stressed the importance of making no major changes to software applications, operational environment, telecommunications, and infrastructure until March 2000.

In its comments, OIT management described numerous positive aspects to SEC's Y2K compliance program which include:

- senior Commission officials including the Chairman were regularly briefed on program status,
- communications between the Y2K team and program offices on their specific systems were held on a regular basis,
- the IV&V contractor role was appropriately increased to address the expanded scope of testing, and
- the goal established by the Chairman for Y2K compliance was met.

Audit Results

I. Certification Process

As indicated in the "Background" section, the certification of systems would occur as soon as practicable after August 31st, 1999.

Based on a sample of 53 mission critical applications, the Commission is making progress to certify its systems. Only seven systems were certified as of August 28, 1999. As of October 22, 1999, the number of certified systems increased to 23. See table for the certification status of the judgmental sample.

Judgment Sample

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 CIS auditor under contract by Office of Inspector General

The certification process entails the preparation of a certification packet by OIT that documents in brief certification recommendations; Y2K test results, exceptions and discrepancies; and forwarding the certification packet for system acceptance by the system owner, Y2K Project Director within the Office of the Executive Director, and OIT's Y2K Director.

In the auditor's opinion the concept behind certification support good management practices. These management practices include: authorization and validation of a system to process in a production status, promoting accountability by identifying and assigning specific owner(s) to each system, promoting an understanding of owner(s) roles and responsibilities over their system and the data it processes. Certification is one of many activities that can be leveraged from the Y2K effort to strengthen the management of Commission information resources for the long term.

Recommendations:

A. The Chief Information Officer (CIO) should continue sponsoring the Y2K certification process of the remaining uncertified systems.
B. The CIO should issue Commission-wide policy to authorize and revalidate system processing by system owners at least once every three years or whenever a major systemic change occurs, whichever happens sooner.
C. Jointly, the CIO and Executive Director should develop and issue Commission-wide policies and procedures to identify and assign system and data ownership roles and responsibilities.

II. Business Continuity and Contingency Planning Efforts

Based on the CIS auditor's limited inquiries to the Y2K Project Director and to OIT management, the SEC is progressing in developing its internal contingency plans. An overall SEC Year 2000 Contingency Plan is being sponsored by the Y2K Project Director within the OED and information technology contingency plans are being sponsored within the OIT. During the audit's field work, these plans were being refined. 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 related to SEC mission-critical applications has been completed and that during November 1999, these plans will be validated and promulgated across the Commission.

The auditor obtained a test analysis report for the EDGAR back-up site (dated September 23, 1999). The test was conducted on August 21, 1999, and based on the test results the EDGAR contractor concluded that the back-up site was properly configured and provides a back-up capability for the production system.

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

Recommendation:

D. The Executive Director and Chief Information Officer should ensure business and information technology contingency plans are tested (*i.e. validated*) as planned prior to the Year 2000.

III. Other Issues

The Y2K project has involved significant resources, much work and many issues. Among them were identification and inventorying of systems, identification of system owners, strengthening system life cycle management (*i.e. change controls, configuration management, quality assurance*), and the development of information technology and business continuity plans.

The accomplishments and benefits of the Y2K effort can and should be leveraged to strengthen overall management of SEC's information resources. The lessons learned from the Y2K effort can be used to develop or tailor practices and guide the development of appropriate policies and procedures in support of best practices. These accomplishments should be maintained by instituting and following appropriate policies and procedures.

Recommendations:

E. To maintain and strengthen the accomplishments brought about by SEC's Y2K effort, the Chief Information Officer should implement appropriate policies and procedures over system life cycle management (*i.e. change controls, configuration management, quality assurance*).

F. The Executive Director and Chief Information Officer (CIO) should ensure that appropriate policies and procedures are implemented to maintain and test business and information technology contingency plans.

Appendix
List of Acronyms

EDGAR- **Electronic Data Gathering, Analysis, and Retrieval**

GAO - **General Accounting Office**

IV&V - **Independent Verification and Validation**

OED - **Office of Executive Director**

OIG - **Office of Inspector General**

OIT - **Office of Information Technology**

OMB - **Office of Management and Budget**

SEC - **U.S. Securities and Exchange Commission**