

This manual was written for the IT auditor as well as for the IT auditee, the individual or group that must prepare for the IT audit. Knowing what the IT auditor or examiner will be expecting gives financial institution management the opportunity to better manage IT risk and establish the necessary internal controls, policies, procedures, systems, and processes that contribute to a safe and sound operation.

It is preferable to address areas of IT risk before the IT auditor or examiner brings the risk to management's attention through audit and exam findings. Such a proactive approach can be a sign of engaged management and a well-run operation. Having the other team's playbook before the big game can help you develop your own winning game plan. Consider this book that playbook. This is not to say that auditors and examiners should be viewed as opponents. Quite the opposite is true. Contrary to popular belief, auditors and examiners do not "get paid by the finding" nor do they enjoy auditing or examining a poorly managed operation.

The best IT audit or examination is one where both sides communicate and collaborate for the good of the financial institution. To that end, we hope this manual gives IT auditors and examiners, as well as financial institution management, the insight and information to complete IT audits and examinations successfully.

The pace of regulatory issuances related to Information Technology was fairly slow prior to year 2000. You had the occasional guidance related to personal computers, contingency planning, and other "easy to identify" areas. IT audits and regulatory examinations could still rely on the Federal Financial Institutions Examination Council (FFIEC) *Information Systems Examination Handbook*. Many financial institutions did not even classify personal computers as "mission-critical" systems. Today, financial institutions could not operate without personal computers and networks.

CHANGES IN IT AUDITING

Thanks to the now-benign year 2000 issue and our new, interconnected, networked world, regulators have geared up to tackle IT issues head on. Clearly, the work done on Y2K planning was an education for regulators and financial institutions' management alike. The issue gave both parties an opportunity to inventory and assess the technology being used by financial institutions. The result was the realization of how pervasive technology has become. Many safety and soundness examiners were converted to IT specialists during the years preceding 2000. Examiner workprograms were beefed up to dig deeper into IT. Many of the questions asked during Y2K exams were simply modified and are now a significant part of most IT examinations.

From the Back Office to the Board Room

Boards of directors have now gained a better understanding of how technology affects the safety and soundness of their financial institutions, and also how they are responsible for oversight. Information technology (IT) is no longer a conglomeration of acronyms and technical jargon; IT is clearly a business issue that is attracting an incredible amount of attention — for good reason. Financial institutions have signifi-

cant investments in technology and due diligence is required to ensure that management makes informed decisions regarding the financial institution's technology partners.

IT Audit Scope Expands

Regulatory issuances related to technology have flowed quickly (see Volume 2). Internet banking, digital signatures, privacy issues, information and network security, to name a few hot areas, have changed the complexion of IT auditing. The audit is no longer contained in the computer room. For that matter, the audit is no longer contained within the institution. Just getting a clear understanding of how all the systems are connected can be quite a chore.

Accordingly, today's financial institution must expand the audit scope to include new areas that are rarely addressed in "canned" workprograms.

CAMELS IMPACT

Back in 1979, the FFIEC adopted the Uniform Financial Institutions Rating System (UFIRS), a numerical rating of 1-5 (1 being the highest and best rating) assigned to the financial institution. This rating, normally referred to as the "CAMEL" rating, and updated in late 1996 to CAMELS, is an acronym for:

Capital, **A**sset Quality, **M**anagement, **E**arnings, **L**iquidity, and **S**ensitivity to Market Risk.

So how does the IT audit affect your financial institution's CAMELS rating? The IT audit, and its related effectiveness, impacts the "M" in CAMELS as management, including the board of directors, is responsible for establishing a sound system of internal controls. An effective IT audit is a significant part of this system.

Increased Audit Coverage

More pressure has been placed on internal auditors to add IT skills to their repertoire. Regulatory agencies that were satisfied with an external IT review every two years and some level of internal IT audit coverage, now demand external IT reviews every year with continuous internal IT audit coverage and greater scrutiny of network security. Some internal auditors have responded to this challenge while others have supported outsourcing the information systems internal audit. Depending on the institution, either approach can be successful. Some institutions are finding that a hybrid solution (e.g., a combination of internal resources plus outside auditors and consultants) is sometimes the best approach to ensure that a comprehensive review of IT is performed.

External resources such as consultants, auditors, and examiners have had to "ratchet up" their skills to meet the demand for the new IT auditor. Many of the old skill sets are simply inadequate as certain areas of IT auditing have become more specialized. It is the rare individual who can perform a comprehensive IT audit on a solo basis. More often than not, a team approach is required.

Making the Transition

This manual has been developed to help you make the transition from the old EDP audit of the 20th Century to the new Information Technology audit of the 21st Century. Some of the old standards still apply and can be used effectively. However, new skills and knowledge must be acquired to competently perform the IT audit.

We go easy on the bits and bytes and offer practical advice regarding IT auditing that you can use. Our hope is that you can use this manual as a guide to customize the IT audit to the unique environment that you will be auditing. Furthermore, we will mix the technical issues with a commonsensical approach to IT auditing that has been well received by financial institutions and regulators alike.

When presenting your findings or making suggestions, your message sometimes gets lost in the “corpspeak,” “auditorspeak,” “technospeak,” or other forms of jargon that cause management and the board of directors to snooze through your exit conference or audit report presentation. Keep in mind that sometimes you have to be a good storyteller and use real-world examples, useful analogies, and at times shocking horror stories to get your message across. To that end, we have provided examples, news stories, case studies, and analogies that we hope you find entertaining and useful.

Regulations on CD

The CD accompanying this manual contains recent issuances from the regulatory agencies that pertain to auditing. The Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of Thrift Supervision (OTS), the Office of the Comptroller of the Currency (OCC), and the Federal Financial Institutions Examination Council (FFIEC) are included to enable you to keep pace with the regulatory matters that concern you and your financial institution. These file are on the CD only.