1-1-1996

Institute of Internal Auditors: Business and auditing impacts of new technologies

Charles H. Le Grand

4

The Institute of Internal Auditors
Business and Auditing Impacts of New Technologies

Charles H. Le Grand
Certified Internal Auditor

New developments in the regulatory, professional, and technology realms are among the most powerful influences on businesses today. As organizations struggle to compete and remain viable in a global economy, management at all levels finds the need for increased skills and new competencies. Auditors too struggle with issues impacting the auditing profession, audit services rendered and the expectations of those relying on audit services.

New technologies introduce powerful capabilities to any staff member. Activities previously reserved for technical experts or skilled clerical staff are now among the growing responsibilities of middle and upper management. Technical details of how enterprise communications systems are set up, monitored and maintained can have major impacts on an organizations continuing ability to stay in business. Thus, it is no longer sufficient to leave such details to specialists, whether this statement is made about auditors or about activities subject to auditing.

THE CONCEPT OF AUDITABILITY

Auditability is a central concept for any process or system wherein it is important to rely on the products or results. To assure auditability a system must provide proof that its results are reliable, and must have features such that an independent, objective review of transactions processed, data stored, and output provided can identify sufficient reliable evidence of continuous security, accuracy, privacy, and availability of information. System auditability features must be required at all levels in an organization and across organizational boundaries in order to extend appropriate assurances to any stakeholder in the organization.

Auditability objectives must be stated by management expressing specific responsibilities for the results of system processing. The auditing profession acknowledges that audit and control concerns extend beyond the realm of accounting and financial reporting to encompass the many issues and subject areas potentially impacting the viability of an organization or the ability to accomplish an organization's objectives. The structure of internal controls therefore must meet control and auditability objectives across a broad spectrum. Auditability objectives for the internal control structure can be identified at three levels: Governance, Assessment and Reporting, and Technology.

Governance

Boards of Directors, Audit Committees, Senior Management:
Senior and board level management expect auditability to assure effective information for governance. Protection of owner equity, public perception, and compliance with laws, regulations and expectations are important governance elements of auditability. The internal control structure of an organization requires the necessary elements to provide assurance at the governance level.

Assessment & Reporting

Self Assessment, Audit Assessment, Management Reporting:
To provide assurance, the internal control structure must include management assessment and reporting techniques that demonstrate controls' continuous effectiveness. Management assessment practices should be authenticated by audits to assure their ongoing reliability.

Technology

Management (all levels), IT Management, Systems Users, Auditors:
The principle application of controls in virtually all organizations today is in the information systems and technology that provide the basis for performing, reporting, and archiving the history of all events and transactions. Thus the principle manifestations of auditability are within the areas of systems auditability and control. The Institute of Internal Auditors Research Foundation provided the necessary research to develop and publish the definitive work in this area known as the "*Systems Auditability and Control*" (*SAC*) reports.

Major Technology Auditability Areas

SAC identifies major technology auditability areas as:
- Information Resources Centers
- Operating Systems and Systems Software
- Systems Development and Maintenance
- Business and Production Applications
- End-user and Client/Server Systems
- Telecommunications and Networks
- Security, Contingency Planning and Disaster Recovery
- Advanced and Emerging Technologies
-

Specific modules and case studies of the *SAC* reports address each of these technology subject areas. This paper addresses some areas where new technologies and other pressures are bringing about organizational changes. It discusses the enterprise impacts of new and emerging technologies. It examines the technology effects on business and technical management, and describes major changes for the auditing profession.

BUSINESS CHANGES RESULTING FROM TECHNOLOGY CHANGE:

New Technologies and Business Practices

Issues arising from current trends in technologies or business practices, and management actions for successful implementation:

Business process reengineering can occur because new techniques are available through practical applications of new technologies. Concurrently there is a need for almost constant retraining of staff in many business areas because new skills and knowledge are needed to use new tools, apply new procedures, and understand new interfaces between management, business peers, customers, and service providers.

New rules for competitive advantage emerge as new technologies redefine the: market place, elements of communication between business partners, components of production scheduling and efficiency, margins for tolerance and profitability, means for information service delivery, definition of timeliness, and much more.

As an example of business changes resulting from use of new technologies, many large organizations will not trade with other organizations unless transactions for ordering, delivery scheduling, billing, and payment processing are all handled through electronic data interchange. EDI processing allows greater control over inventory management, manufacturing processes, delivery schedules, cash management, human resources, and other business elements. Standards for

EDI transactions, processing and communications protocols are somewhat mature and well documented although such standards are not universally accepted. Use of EDI includes specific risks as well as new control and auditing tools.

By eliminating unnecessary processing steps, time delays, warehousing, spoiled goods, and other costly factors, a provider of products or services can reduce prices and redefine the rules of competitive advantage. EDI and other forms of electronic commerce are reshaping processes from acquisition of raw materials, through processing and distribution, to retailing and settlement of financial transactions. Entirely new business relationships are defined through the redistribution of responsibilities between manufacturers and retailers, eliminating wholesalers and warehousing, and assuring availability of goods when and where needed. These new relationships both take advantage of, and rely heavily on the interface of diverse systems coordinated via networks, accomplishing both common and disparate objectives.

New devices and techniques in the marketplace not only automate the processing of previously time consuming, sensitive, tedious, and error prone manual activities such as cash register operations, but also provide data directly usable by numerous related operations. For example, scanners at retail counters can provide data for daily sales analysis, customer history, inventory management, manufacturing and distribution forecasting, trading partner financial settlements, analysis of marketing campaigns or promotional pricing, determination of seasonal or geographical fluctuations, and more.

Control, Security and Auditing Issues

Major control, security and auditing issues relevant to technologies and business practices, and techniques for addressing them:

Migration of Controls and Security: As systems change in scope and employ new technologies, the location and purposes of controls tend to migrate to new system elements. At one time controls were centralized within the central computer and all the various control elements related to the centralized control structure. As application system capabilities expanded, certain controls migrated into applications. As database management systems matured some controls migrated to the DBMS environment. Each new element added to a system has the potential of altering the location of important controls and possibly subjecting them to varying degrees of reliability.

Modern computing environments are most often characterized by the network as the central element with individual computing devices on the network identified as servers, clients, or both. The former central computer system is now just another server on the network. Network security is a key element of system control, and trust relationships must be defined for networked devices, users, and even business partners through features of the network operating system and its interface with other systems and networks.

The security and control of any computer on a network is dependent on the privileges provided to trusted users and to access rights and trust relationships defined for other network devices and remote users. Security of networked systems is also dependent on the systems' ability to defend themselves against unauthorized access. Security and control elements are implemented through a variety of system features that often are immensely complex and esoteric to a specific environment of brand named hardware, software and network components. Security and control components may reside within operating systems, network components, specialized systems software and hardware, database management systems, program objects, application systems, and many other locations. Security within networked systems may be dependent on the "weakest link" within the network because of the inordinate expense of individually securing each networked component

against all potential breaches of security that could occur due to control failures within other components of the network.

Centralized Controls Administration: As systems and system components are distributed across diverse environments, it becomes ever more important to centralize the administration of security and control within an organization. The organization's central control group must be responsible for prescribing and administering effective control practices across all organizational elements. Centralized control must also administer controls over communications with entities outside the organization (such as business trading partners communicating over a value added network, and other outsiders with a vested interest in the integrity of information provided). Obviously staff resources in such a group need strong expertise in systems technology and business controls as well as the ability to deal with personnel across organizational boundaries and at varying levels of management.

Security and control guidelines must be consistently applied to all systems regardless of size, location, technical complexity, or number of users. A seemingly minor system running on a personal computer can be a point of entry to other systems on the network. But security guidelines are also restrictive in nature and must be tailored to appropriate business practices in the immediate areas to which they apply. Thus the centralized control group must be sensitive to risk management issues and cost effectiveness of controls.

Management Responsibilities for Controls: More important than the features of the operating systems, networks, or even the application systems are the organization's policies and management's attitudes about security and control. An inherently insecure system can be secured within an environment of effective controls. The most secure systems available can be compromised by ineffective application of systems environmental controls. Therefore it is important that management at all levels be provided the knowledge and tools needed to assure consistent and effective application of controls.

The application of technologies such as those found in client/server systems and networked environments requires new rules for such traditional controls as: separation of duties, security and access protection, data administration, software distribution, and backup and recoverability. Often members of management responsible for meeting control objectives are not familiar with them and lack appropriate guidance in their implementation. Management not familiar with traditional systems risk issues may be first unaware of the risks, and second unable to identify appropriate control techniques when risks are identified. Transversely, management not familiar with new technologies may prescribe ineffective control techniques based on obsolete knowledge of systems design features and components.

Control objectives have often been expressed in terms of traditional system features and personnel assignments. For example, the separation between programmers and production systems operations was initially required to reduce the likelihood that individuals who understand system features could cover up errors or fraud through access to live transactions or software, or disclose sensitive information. In a client/server environment there are new requirements for separation of duties as one person may perform the tasks of system design and development, programming, testing, computer operations, transaction processing, error correction, reviewing of system results, and storage of history records. Thus separation of duties must be defined at a level that will provide detection of unauthorized activities by some other business unit operating under a separate control structure.

Assessment of Control Objectives: Controls must be designed to do more than reduce risk. They must provide an environment of effective control at reasonable cost. Therefore managers must be

alert to new system features that can allow the elimination of expensive or complex controls in favor of more cost effective control techniques. Management actions to provide an acceptable level of risk should take into account economies of scale and the relative costs of preventing versus detecting and correcting errors.

Controls can be applied using a variety of techniques, and new technologies can change the factors used to evaluate the cost effectiveness of controls. For example, the cost of continuous control monitoring or auditor use of expert systems technology may have been prohibitively expensive in all but the largest systems environments just a few years ago, but may be regarded today as attractive alternatives to sampling or after the fact analysis.

Control self assessment should be a cornerstone of ongoing assurance of internal controls. This implies an effective self assessment process as well as the auditor's assurance for systems and activities subject to control. The organization's internal control structure must be a cohesive and comprehensive system as described in the COSO report, "Internal Control - Integrated Framework" published in 1992. The COSO report acknowledges the importance of information systems controls and refers to the *Systems Auditability and Control* reports for appropriate detail. The *SAC* reports specifically address business and technology risks, control objectives and techniques, and the roles of auditors in assessing overall systems security and control.

The auditor's first task in assessing system security is to examine the controls environment for the organization and determine whether the practices enforced are supportive of reliable computing. If so the auditor may proceed to examination of specific controls. If an effective control environment is not enforced, then the auditor will proceed to examine areas of greatest known exposures, and conduct tests to identify the extent to which systems are at risk.

Auditor Involvement in Developing Systems Controls: In times past, management hoped to rely on auditors to provide the level of expertise needed to assess the adequacy of controls designed for new automated systems. Unfortunately there are at least three flaws in the theory that auditors can provide the needed controls expertise for new systems designs:

1. There are not enough auditors to participate in all significant systems design and development projects. This condition is exacerbated in the proliferation of distributed, client/server, and networked systems acquired, developed and implemented outside of a central information systems group.

2. Reliance on auditors to specify control objectives and appropriate techniques removes the responsibility for controls from those designing the systems and those who will use them when they are completed. The education of systems designers, developers, and user management, as well as auditors, in the areas of risk management and application of controls is essential to ensure the ongoing effectiveness of future systems development and implementation. Auditors must not accept responsibility for controls design and must avoid activities that give the appearance of being responsible for defining controls. Using auditors to specify controls impacts their independence and objectivity. Section 100 of The IIA's Standards for the Professional Practice of Internal Auditing states that "INTERNAL AUDITORS SHOULD BE INDEPENDENT OF THE ACTIVITIES THEY AUDIT." All auditing standards have similar provisions.

3. While it is appropriate for an organization to wish to take advantage of the auditor's controls expertise to prevent mistakes in systems design and implementation, there are significant problems in trying to skirt the independence issue by planning to use other auditors to perform subsequent audits after a system is completed. The worst of these problems are presented as

issues one and two above. Significant audit expertise is needed to evaluate the organization's methods for developing and implementing systems. The systems development processes are themselves a system which produces other systems. Until the auditor has addressed the issue of how controls are designed into all systems it is fruitless to attempt to assure controls are designed into individual systems. Indeed an organization would be well advised to provide assistance to the internal auditing function while new systems are being designed to help identify systems features that will improve their auditability and provide continuous real time or soon after the event monitoring, error prevention and detection and other important controls.

An organization's security and control guidelines must specifically address auditability and control features and capabilities, provide specific guidance, and include audit considerations for all automated systems. Security and control guidelines should be examined by the auditors to assure they are appropriate given the operating environment, and will provide a reasonable baseline for individual system audit assessments.

The organization's auditors may or may not be involved in developing security and control guidelines for any given system or operation, but should assure the element of auditability is clearly understood by those responsible for providing and implementing the guidelines, and that auditors are automatically included as users of systems auditability features. Auditors then should examine proposed auditability feature designs for major new systems or revisions and assure the tools and techniques identified will be appropriate.

Continuous Control Monitoring and Continuous Process Audit Systems: As many systems process extremely large volumes of data including sensitive transactions with tight time constraints for preventing, detecting and correcting errors, many traditional audit techniques such as sampling or annual assessments can no longer be effective. Therefore auditors are using continuous control monitoring (CCM) and continuous process auditing systems (CPAS) to alert them to potential systems problems in time to take appropriate actions.

CCM and CPAS techniques can monitor data for transactions or events and compare them against expected criteria for such transactions or events. If data patterns indicate anomalies or known error conditions, the related transactions and supporting information can be captured and reported to the auditors for investigation. If a data anomaly is determined to represent an unusual but legitimate series of events, then the system's experience base or analytical rules can be modified to recognize such events in the future. Artificial intelligence or expert assistance features built into systems can improve their ability to identify anomalies and known risk or error situations, capture relevant information, and alert management as soon as a problem is detected so they can address problems before they get out of hand.

Use of CCM or CPAS as audit tools will likely raise the demand for controls of this type for use by managers as they will not want the auditors to know all the details of their problems before they even know the problems exist. Thus, an effective means of improving the overall state of systems auditability and control is for auditors to use advanced technologies and then share their techniques with management in the areas to be audited.

There has been some speculation that the use of advanced control and security techniques including CCM, CPAS, and artificial intelligence will lessen the need for auditors. However, until human nature changes and people stop making mistakes, there will always be a need for independent assessment of the reliability of systems and information. The auditor's job will, however, require the application of sophisticated knowledge and techniques as future audit tasks will include the validation of built in system audit features and the assessment of the general controls that assure the continuous effectiveness of such features.

Technical Details Integral to Control, Security and Auditing

Technology impacts on business practices, management issues, control, security and auditing issues.

As controls migrate into and among new technology system components, with the related impacts on business and management issues, new rules for assessment and attestation will change audit practices as well as the purposes and expectations of audits.

Some of the key enabling technologies applied in systems today include distributed systems, object technology, internetworking, expanded storage, and intelligent systems. Few technical systems experts can be expected to comprehend the complexities of this small but meaningful subset of new technologies. Even fewer can be expected to understand how they relate to each other and the collective impacts on controls resulting from their simultaneous implementation within an organization. Yet as new technologies are implemented within every component of an organization, the auditor is expected to: use appropriate judgment to evaluate and assess control strengths and weaknesses; design and conduct meaningful tests and evaluate test results; and render opinions on the validity of financial information, the integrity and reliability of other information and systems, compliance with laws and regulations, and any number of other expectations wherein independent assurance is valuable. Clearly the expectations of auditors and their ability to deal with both broad scope issues and extreme technical details are increasing.

The experienced auditor who can address modern business systems is in great demand. However, even the best and most technically competent auditors cannot know everything about new technologies and cannot examine all the significant risk components for an organization's systems. The following sections address some of the intricacies of new applications of technology and how knowledge of the systems described is important to the audit function. Also addressed are the interactive roles of auditors with the management responsible for implementing new technologies and with those responsible for or relying on system processing results.

ENABLING TECHNOLOGIES

The availability of inexpensive yet powerful computing and network components enables the implementation of client/server systems and local area networks as well as many other new applications of technology. The structure and techniques of both business and technical controls in these environments are dramatically different from traditional controls. Further the controls rely heavily on technical components that may be difficult to understand, are subject to constant change, and may be based on emerging standards or no standards at all.

Assessing the integrity and reliability of client/server and LAN based systems and attesting to the validity of information produced from such systems represents significant challenges to management, auditors, and technology professionals. Fortunately the level of interest in controls and auditability of systems is increasing in both the providers and consumers of such systems. Security, control and audit guides have begun to emerge as critical components of systems being considered for acquisition. However, much of the implementation of client/server and LAN based systems uses custom combinations of individual components from a variety of sources and a range of services from independent providers. Further, audit appraisals of such systems are often based on first time reviews of unfamiliar technology using tools and techniques that may also be new and/or unproven. Specific management and audit challenges addressed below are excerpted from the 1994 "Advanced Technology Supplement" (Module 13) of the *SAC* reports.

Client/Server Architectures

Implementations of client/server systems take advantage of enabling technologies that provide modularity, portability, interoperability, and flexible communications between system components. Technically speaking information processing, storage, and interface with system users can be applied cooperatively across a mix of interconnected processors in a client/server environment in a logical versus physical architecture. Thus it may be difficult to identify a specific machine or processing environment where a critical system component resides, and the architecture may change dynamically based on the availability of versus demand for processor cycles, storage capacity, or communication bandwidth. The considerations of security, accuracy, privacy, availability, auditability, etc. are directly impacted by technical issues of design, capacity, scalability and performance.

Evolving Management Issues related to client/server systems implementations include:

- Training of information technology and end-user staff - Training includes use and application of new tools, functionality, responsibilities, languages, operating systems, user interfaces, etc.
- Planning the migration - Migrations to client/server technology may include new approaches in budgeting, use of support staff and/or consultants, new roles and responsibilities, etc.
- Dealing with multiple vendors - Separate vendors may provide hardware, software, networks, network services (i.e. VANs), consulting, conversions, implementation, testing, etc.
- Packaged products and application enablers - The rush to develop new products may result in components that lack functionality or perform inconsistently, thus increased attention to specifications and testing is important although personnel may lack such expertise.
- Benefits of successful implementations - While significant benefits such as improved work flow, reduced cycle time, reduced costs and greater availability of information are possible through client/server technology, it is important to assure the benefits are real and are not traded against negative impacts such as decreased reliability or control.

Control, Security and Auditing Issues for client/server technology are similar to those for other environments, but the tools, techniques and audit approaches may be dramatically different:

- Development and implementation of client/server platforms employ new approaches that may be unfamiliar to management and auditors yet may occur simultaneously across broad segments of the organization for both mission critical systems and those of lesser importance.
- Management of transaction processing in a distributed environment may include execution across a network of distributed systems involving multiple transaction types processed locally on a particular client or server system. The system transaction processing control features should support discrete, consistent, isolated, serialized, and durable characteristics. These are provided by such technical controls as transaction identifiers, checking the status of all participants to a transaction, executing a two phase commit algorithm, detecting and resolving deadlocks, and coordinating transaction recovery.
- Management of data and process workflows may involve new or unfamiliar data management techniques such as snapshot, replication and fragmentation. Data distribution is dependent on the intended use, is implemented via distributed data management techniques, and will affect such control considerations as administration, access and currency.
- Securing the environment is a complex task due to the number of access points, the concurrent operation of multiple user sessions, and extensions of data access and update capabilities. System access points must be examined both individually and collectively.

Technical Perspectives: Security, control and auditing of client server systems are complex and subject to constant change.

Multi-tiered client/server environments are structured to support cooperative processing and to provide flexible domain and workgroup definition. Scalability is an important design consideration as are the features supporting graphical user interfaces (GUI), message passing concepts and remote procedure calls. Networked structured query languages provide a particular environment supporting requests and associated data from one process to another which may include clients and servers residing on different systems possibly under different operating systems. As the client/server environment employs distributed database and/or transaction processing functionality it is also common to use an intermediate software layer (middleware) that provides connectivity and unification services to remote sources of data or coordinates transaction processing among distributed and often heterogeneous servers on the network. In such environments network interface administration becomes a critical system control that should be subject to constant monitoring and frequent audit attention.

Local Area Networks

LANs and LAN based systems are subject to most of the same management, control, auditing and technical concerns as client/server systems and in many cases are components of such systems. Additionally there are some specific concerns related to the use of LANs in an organization.

Evolving Management Issues: LANs are rapidly becoming one of the most important components of the organization's internal control structure. They are expanding in size and speed, and provide processing for applications critical to business success. Through connections to other LANs, networks and platforms, LANs are becoming extensive repositories of production data and programs. They are also becoming the testing ground for new applications of technology and new interfaces between business functions.

LANs are becoming the central nervous system for businesses as they link together important components both within and outside the organization. For IT managers LANs may also become the center for their anxieties as LANs are subject to disruptions with effects ranging from minor annoyances to catastrophic results. Fault tolerance and security features are often added after a network begins to mature rather than during initial implementation. Network management is dynamic as both the technologies and business uses of LANs change continuously.

A primary incentive for installing a LAN is to share and consolidate information resources otherwise confined to single systems or stand-alone user groups. Both opportunities and risks are introduced as LANs facilitate data sharing, improve communications and cooperation, reduce processing time, and allow redeployment of resources. The system components allowing these changes also change rapidly thus relocating system processes, capacities and controls.

As organizations downsize, merge, expand, or otherwise change, network administration must keep pace with the changes. Ideally all subdivisions of an organization would conform to computing and network standards. In reality system types typically are diverse and the interconnecting of LANs is both complex and costly. Internetworking introduces management and control concerns that can impact the integrity of systems and information.

Networks connect more than just computers and peripheral devices. They support workgroups sharing, hopefully, common objectives. System applications supporting workgroups can actively control the flow of work between departments improving the overall control environment. Faster and bigger networks and the mixing of LANs with WANs (wide area networks) and the Internet continue to provide enhanced communication and processing services. Electronic commerce over

open networks is a pioneering activity to most organizations and will introduce significant new opportunities as well as new threats and risks.

Control, Security and Auditing Issues: LANs are not yet a mature technology. Most LANs were originally designed and implemented to be more open than secure. Mission-critical applications have migrated to LAN based systems. And a combination of interlocking techniques is required to provide an acceptable level of control for LANs.

Organizational considerations for LAN security and control arise because nontechnical people with little or no specific training find themselves responsible for fundamental computer security and control, network administration, and other issues that merit attention at the organizational policy level but may never have been addressed. New working relationships are formed among departments, and potential conflicts of interest and other control concerns can arise. Appropriate remedies for these concerns include: senior management support for security initiatives, development and enforcement of pervasive security policies, periodic security awareness programs, specific security responsibilities in LAN administrator job descriptions, specialized security training for LAN security administrators, centralized LAN security management, and effective auditing of LAN security management. (Such issues will likely be addressed in generalized audit questionnaires for computer security and control but may not directly apply to the LAN and interconnected networks environments. Thus customization is needed within the audit approach and training may be needed by technical auditors to address LAN audit concerns.)

Logical security, potentially impacting the entire organization, may be implemented at the network level. Historically logical security was provided at the application level or within specialized systems software. Changes needed in logical security or related control techniques were required to go through established change control parameters and procedures. Networks today and tomorrow provide the mechanisms to restrict or allow access to individuals or groups based on complicated control parameters. LAN security controls may also be the first line of defense for virus protection, enforcement of software copyright provisions, and other controls.

Operational network management issues, network software change control, continuity of processing and contingency planning, and physical security are all traditional controls migrating to new homes within networks and client/servers systems. Again the management and audit approaches to such controls will require constant attention due to the volatile environment.

Technical Perspectives: Management and auditing of LANs includes the need to understand the underlying enabling and supportive technologies providing improvements in LAN speed, performance, enhanced network data handling, and value for money. New technologies are the bases for bigger and faster networks, and will significantly impact network topology, management, security, control, and continuity of processing.

Increases in speed and network data handling result from both improved network components, such as fiber optics, and from new uses of existing technologies such as Copper Distributed Data Interface (CDDI) and fast ethernet over existing twisted pair and coaxial wiring. Optical fiber is inherently more secure than copper wiring, so concerns for speed and cost effectiveness may also be impacted by control concerns. The need to carry voice, data, images, and even video over LANs is expanding. Technologies supporting such capabilities include Asynchronous Transfer Mode (ATM), Switched Multimegabit Data Service (SMDS), and Frame Relay. Standardization issues for these technologies are impacted by the telecommunications industry perhaps to a greater extent than the concerns of LAN users. Nontechnical managers and auditors may be only peripherally aware of the technical and/or standards issues in network management.

Network management tools that allow continued growth and increased performance also include some highly technical components. However in order to distribute control of LAN administration to nontechnical staff, management, operational and problem solving tools must be easy to use and powerful enough to include network configuration, administration, monitoring, problem detection, analysis, and repair.

Interconnectivity among LANs and with other networks is required and increasing in most organizations today. Sharing information resources across different computer platforms, merging organizations with dissimilar technology, and the need to access information outside the organization are some of the many reasons for interconnectivity. For the network manager, and the auditor, each connection provides a possible failure point for security, operational efficiency, continuity of processing, and contingency planning.

Competing communications protocols, internetworking devices such as bridges, routers and firewalls, variations in network operating systems software, and the potential difficulty in even identifying the source of network-based services are among the many technical issues facing LAN managers and auditors. Fortunately the technology vendors are beginning to take a more active role in working with the security and auditing professions to not only provide better security and control features and options, but to also better explain their use and to reduce the amount of risk inherent in systems used with only the default features activated.

EMERGING TECHNOLOGIES

Numerous advances in technology are impacting business in new and often unanticipated ways. In addition to the obvious benefits of the technology there are also new control concerns and new opportunities to improve security, controls and auditing. Anticipation and advanced warning are two important elements to assure auditors will be in a position both to positively impact the auditability of new systems and to develop the expertise needed to audit them. Training and participation in the analysis of emerging technologies is essential to the future effectiveness of the auditing profession and the individual practitioner.

Object Technology

Important changes are occurring in the definitions of basic parts from which software applications are constructed. The great hope for object technology is a dramatic improvement in software development through the reuse of standard software parts rather than the reinvention and reconstruction of the same parts in every new application.

Enterprise impacts of object technology should be realized in improvement of the design, development, testing, implementation and maintenance cycles for systems. Also object technology may shift the organizational placement of systems analysis and programming activities. Libraries of trusted and audited software objects may be prepared and maintained under conditions roughly equivalent to traditional systems development and subject to equivalent controls, but the use and reuse of these objects may be available to virtually anyone in the organization with a need to produce information from available data.

New systems can more closely simulate actual business processes as, for example, workflow software may visually and explicitly depict the manner in which financial transactions are processed. Graphical instrumentation for financial and business procedures can also provide managers with more specific and more intuitive information about decisions they make.

Applications will be easier to use and modify as software objects are combined with point and click tools allowing them to be used with the same relative ease as PC spreadsheets and databases. While software professionals will be needed to cultivate collections of useful objects, users will be able to assemble objects in novel and useful ways.

New skills are required for systems developers using object technology as new techniques as well as new problems emerge. Significant changes in control concepts are emerging in both the technical and user arenas. New tools reputed to be self documenting will fall short of this expectation. Rapid application development and prototyping will sometimes be used to rationalize gaps in requirements analysis and system design to the detriment of software quality.

Object technology will also provide opportunities for new auditing approaches as object tools are combined into software development environments and standard control and audit objects can be included into tool libraries for both programmers and auditors. For example, an embedded expert audit object could alert the auditor when conditions are identified in a CASE (computer assisted software engineering) repository of system specifications that fall within the parameters of systems selected for specific audit attention. The auditor could then take steps to address auditability features while the system is being designed.

Technical overview: Information about object technology is important to understanding why this technology is significant to new directions in security, control and auditing. The anatomy of an object differs significantly from traditional programming. Software objects combine both programming instructions and data manipulation into the concept of an object. Traditionally data and processing components have been separated which provided an important control technique.

Classes, instances, subclasses, and inheritance are new concepts in terms of how software objects are designed, categorized, used, reused, and structured to accomplish system tasks. Object languages take into account the different messages that may be passed to an object, and the source of such messages, to determine the actions to be taken. Storage systems too change as object oriented databases facilitate the combining of data and the instructions needed to process that data in a logical structure to interface properly with physical device and network features.

Design methodologies and new concepts in development tools introduce opportunities to refine systems development methodologies. However these methodologies are not mature and there is a general lack of precedents for estimating object oriented development tasks and schedules. Auditors may find the need to specifically address object development methodologies to assess the development and use of reusable objects, class libraries and frameworks for object and data management, analysis and design, testing, documentation, and object change control.

Distributed objects combine the techniques, as well as the risks, of managing object oriented systems across distributed client/server environments. The challenge is to package software in self contained modules that can then be transported in some secure manner to other machines for processing. Distributed processing provides a severe test of standards, either proprietary or open.

Object technology incorporates new features not necessarily intuitive to those experienced in traditional programming languages and approaches. Auditors should understand these features and their benefits to provide the insight needed to specify auditability features for systems standards and specifications. Object concepts also have significant implications for system testing and documentation and controls for these important functions.

Open Systems

The paths to open systems are based on the desired features of interoperability, scalability, portability and compatibility. These features are provided through development of and adherence to open systems standards. There are significant benefits to be gained through development and implementation of open systems standards, but as in any standards oriented issue there are also the concerns of which standards to follow and how standards will be impacted by technology innovations.

Enterprise impacts of open systems can depend on the organization's flexibility and the existing investment in legacy systems. Investments in technology and systems applications will impact the organization's approach to migrating toward open systems environments. Open systems concepts may be based on either public or prevalent standards. Either way there is no assurance today that such standards will long endure.

UNIX systems are a good example of proprietary and industry standards and how they do and do not work together. As an open system, UNIX should support portability of software and systems across platforms and different vendor systems. However there are many proprietary versions of UNIX and there have been many UNIX standards setting initiatives. UNIX today is a collection of individual operating systems specific to individual vendors and designed to run on specific processors. Applications for UNIX may be specifically designed for portability across platforms, by avoiding vendor specific enhancements to features or even controls, but even so it will most likely be necessary to recompile programs as they are moved to another UNIX environment.

The role of open systems in distributed processing is to promote the interoperability of processes across diverse environments. However, open systems do not happen automatically or overnight. Auditors should be on guard to assess the effectiveness of management actions to plan and implement open systems as well as to prepare the organization to manage them.

Technical Overview: Open systems include three layers of architecture. It is important to understand the components making up each layer because of the impacts changes in them will have across any given organization and its dependence on open systems architecture.

Layer 1 - Computing hardware is the foundation for systems. It is profoundly impacted by advancements in the microprocessor arena. Standardization at this layer is primarily de facto and is driven by the large investment needed to sustain a presence in the industry. Standards are also impacted by consortia among industry leaders.

Layer 2 - Operating environment provides the interfaces to the hardware and application layers. This layer is highly volatile and includes operating systems, graphical interfaces, system software, and network protocol. Open operating systems today are designed with a layered approach to accommodate changes in either layer one or three via standard interfaces. Layer two software developers have also begun to recognize the importance of security and auditability and have taken steps to work with the auditing profession to define and document security, control and audit guides for their products.

Layer 3 - Application enablers include computing languages, CASE products, database management systems, and packaged software. Packaged software is by nature proprietary so there is little openness at this level. Some vendors are beginning to see advantages to building packages that can share information across applications. These packages still tend to be proprietary and typically are designed to give the vendor some advantage over other vendors.

Auditors who are able to address security and control issues across open systems also tend to specialize in specific packages and environments. Auditors using audit software in open environments must also address the issues of portability and scalability and can be more effective in organizations where management has a high regard for the value of organizational standards.

Multimedia

The emergence of multimedia tools and the rapid acceptance of these tools in the workplace is changing the nature of the work, the forms of information, the concepts of control, and the techniques whereby an organization interfaces with suppliers, customers and partners. Multimedia also changes the nature of evidential matter used for control and audit assessments.

Enterprise impacts of multimedia will tend to motivate the acquisition and creation of this technology over time and the pace of change will increase as the technologies become more affordable and more widely used.

Multimedia involves the combining of two or more of three specific elements: moving pictures, sound, and graphics. Text is assumed to be included in multimedia although it may not be an essential component as systems combine voice recognition, magnetic stripes, universal product coding (UPC or bar codes), touch sensitivity, and other means of communicating without necessarily using any specific written language. As audit evidence has traditionally been based on text and numbers in human or machine readable form, the auditing profession will have to closely follow developments in multimedia as records of auditable transactions and events migrate to these technologies.

As organizations transition to more powerful user workstations, sound and CD-ROM are often included as standard features. As the Internet and World Wide Web (Web) are exploited as new tools for gathering and distributing information, multimedia becomes a de facto standard. As multimedia becomes an accepted component of business communications there is greater demand and increased requirement for telecommunications capability with increased bandwidth to cover the increase in size of messages transmitted.

New applications in sales and marketing emerge as customers are reached via the Internet or other multimedia applications. Thus it is essential for auditors to have specific knowledge of the factors impacting the feasibility, use, control, security and auditability of systems using multimedia components. New techniques for securing transactions across open networks will likely be resolved first for text transactions and then transition to nontext communications. (Although encryption, for example, is already widely available for voice communication.)

Technical overview: Multimedia systems require additional hardware and software components to support audio, graphics and video. Multimedia development should follow typical system development controls taking into account business and technical feasibility, user requirements, hardware and software vendor stability, and the extent to which industry standards exist.

Technical approaches to assessing controls over multimedia implementation can involve reviews of new input and output media, new forms of storage and storage media including new techniques for data compression, and new systems software components. While the involvement of auditors in reviewing multimedia systems may not seem important because early systems are likely to be of a non-critical nature, these early implementations may set patterns and control standards for subsequent mission critical systems.

As tools for communicators migrate into multimedia it is important that promotional staff and other communicators be brought up to speed in these technologies. Advertisers today who focus exclusively on developing printed ads and brochures are instantly obsolete when the organization shifts its marketing objectives to include use of video, audio, the Web, and other multimedia techniques. Many organizations today are scrambling to provide a multimedia infrastructure as employees develop new tools and approaches such as preparing Internet or intranet Web pages.

Intelligent Systems

Artificial intelligence and/or expert systems (AI/ES), when successfully applied, may be invisible or nearly invisible in the business functions using these technologies. People often think a system should have greater intelligence than to create the results they see. ("Why would they do such a stupid thing?") But they may not understand the complex relationships between data, rules, and analytical techniques which make systems perform more intelligently or the challenges inherent in increasing the state of intelligence in systems.

Enterprise impacts of AI/ES should be understood by management in order to recognize areas where the organization depends on specialized expertise and determine if AI/ES could be applied to an advantage. Potential areas for AI/ES application include: expertise and performance bottlenecks, functions with high training costs, and activities dependent on characteristics of large volumes of data as in forecasting or monitoring of unusual transactions or events. AI/ES techniques are made available and feasible through advances in the technologies of data management, faster and cheaper processors, and improved analytical programming techniques.

AI/ES can provide increased sharing of experience through encapsulating that experience in the programmed rules and structured data of a knowledge base. Decreased dependence on human experts may be a desired result of AI/ES especially in areas where expert assistance is needed by a larger group of people than can be served by the available number of human experts. Taxation knowledge is an example of specialized expertise needed by a large body of people (tax payers and auditors) who are not necessarily tax specialists. Because of the large body of highly specific rules, taxation is a good area for AI/ES. However, shifting the dependency on expertise from humans to systems provides both opportunities and the responsibility to assure such experts perform reliably.

Greater leverage of historical data may be provided if AI/ES techniques are applied against such data. Increased productivity and competitive advantage are other potential incentives to invest in developing AI/ES. In any case the application of this technology creates another area subject to validation and auditing as such systems may be, or soon become, mission critical.

Technical overview: Expert systems use facts, relations, and heuristics expressed as rules and frames, and therefore are declarative. This is in contrast to conventional programs which are based on explicit control over the sequencing of operations and therefore are procedural. A variety of tools, languages and techniques are available for constructing expert systems ranging from extensions to general purpose programming languages to highly structured software environments called "expert system shells." Applications that are natural candidates for AI/ES are those where the human decision making process can be seen to follow a set of rules that can be articulated. Examples include review of insurance or loan applications or insurance claims.

Specific technologies applied in AI/ES include neural networks and fuzzy systems. A brief description of each may help explain why understanding of these technologies may be important to auditors. Auditors charged with validating the results of such systems will need much more than a cursory understanding of the technology.

Neural networks are built from historical data describing a situation and its outcome. Neural networks are pattern detection schemes, a point made clearer with the following example: Graduate students in a UK university constructed a general purpose coin box using neural networks. There is a slot for the coin, a sloping ramp where it rolls down, and a wall where the coin collides and stops. The data for this system are obtained from a microphone that listens to the coins drop. Over repeated trials, as a coin is put into the box the sound of its drop is digitized and the identity of the coin is revealed to the software. Eventually the neural system
is able to discriminate among coins by detecting patterns in the acoustical data.

Neural networks are built from elements that each behave somewhat like individual nerve cells (or neurons). Each neuron can be thought of as a single, simple processing unit. Large numbers of neurons linked together in densely interconnected layers form a neural network. Some neurons are sensors that receive input from the user or the outside world, others are effectors and are the output of the network. Nodes are linked mathematically. When input data are presented to the model, calculations lead to an outcome or conclusion. Each neuron in a neural net receives signals from some number of sources or other neurons, and sends a signal on to others. However, in determining the signal it sends on, it can weight each of its inputs to reflect how much attention it is paying to that input. Neural networks "learn" by adjusting these weights, which can be thought of as representing the strength of the connections between individual neurons. Training algorithms incrementally change the interconnection strengths between many pairs of neurons until the network gives correct answers for a set of training data.

Fuzzy systems contain programs with variables whose values are expressed as a fuzzy set. Elements of the fuzzy set carry weights to indicate their degree of membership. Degree of membership indicates the extent to which an element conforms with the overall premise of the set. For example, 35 and 45 degrees Fahrenheit may both be members of the set "cold temperatures," however, 35 degrees would have a higher degree of membership. Calculus is often used to compute the weights of the fuzzy set in the "fuzzification" phase. These weights are applied against a predefined rule set to determine the strength of output results. Additional calculations are then performed to resolve vague or conflicting results during the defuzzification" phase. The output of this phase is a concise final result.

Fuzzy systems consist of: A rule base; a fuzzy set (i.e., data describing the imprecise environment such as cold, cool, warm, and hot, or low, medium, and high); input data (e.g., temperatures); and degrees of membership (i.e., the strength of relationship between each input value and each fuzzy set value).

Auditing implications for AI/ES are based on the fact that applications of this technology are increasing and having important impacts on many organizations. In the course of audit assignments the auditor may find a need to increase or acquire technical understanding of expert, neural, fuzzy or other intelligent systems to address control, security and audit risks. An audit engagement may require the auditor to: ensure sufficient and accurate base data are accumulated for neural networks; ensure procedures are in place to update neural networks as new or revised data become available; and consider legal implications of reliance on intelligent systems for business decisions making purposes. As organizations expand their use of AI/ES, internal auditors may find it important to maintain active involvement in expert systems development and to evaluate whether intelligent systems might add value to the auditing function.

IMPACTS ON INFORMATION TECHNOLOGY MANAGEMENT

Emerging technologies bring about significant changes in the processes employed within IT functions as well as the relationships of IT with other elements of organization management, governance and auditing.

Strategies and tactics for planning and managing systems change as the roles of system design, programming, analysis, operations and other traditional IT functions are distributed to nontechnical areas of the business. IT historically has been perceived as a bottleneck in many organizations inhibiting the expansion of new systems due to the scarcity of systems personnel and huge project backlogs. In distributed systems environments IT personnel may still be the scarce resource that is consequently unable to provide structure to the explosive growth of systems and networks throughout the organization. IT specialists may then be called upon to provide support and troubleshooting for systems over which they have no control and with which they have no experience. Incompatibility among networks, data structures, software packages, electronic mail systems, communications protocols, and many other technology components are some unfortunate potential side effects of user controlled growth in distributed systems. IT typically inherits the challenge of recombining disparate systems into the cohesive framework needed to support business continuity and growth.

Relationships with technology vendors may shift in organizations where IT is not involved in a centralized control over acquisition of systems resources. In addition to the incompatibility issues mentioned above, an organization may lose benefits of bulk purchasing and favored status from suppliers who know the volume of business associated with large customers.

Skills required by application developers change significantly with the introduction of new technologies such as those described in this paper and the *SAC* reports. Roles for a distributed base of systems users and managers must be defined not only from a technical perspective but also in relation to the policies and procedures needed to protect the organization from new risks such as those brought on by software piracy, invasion of privacy, and introduction of viruses.

The cost structure for feasibility of systems design, management, and maintenance is in constant flux as technologies emerge and mature. The organization's strategies of employing newer versus more mature technologies will also affect the decision processes for technologies, applications, and techniques to employ.

Dependencies on systems components shift as new functionality is added to systems and networks. Network firewalls which previously were obscure components of highly sensitive or secret systems are now critical elements of networks allowing or preventing remote access. Firewalls may also be single points of failure potentially impacting the entire organization if they have not been incorporated into the business recovery plan.

IT management must continuously assess security threats and vulnerabilities from an enterprise perspective. The move from well controlled centralized mainframes to decentralized and distributed desktop and client/server environments has a huge negative impact on security. Rather than controlling security for systems environments IT must encourage and promote participation of the security function in technical and operational initiatives.

Methods for authenticating systems users and their activities may not be standard options in systems selected to satisfy operational objectives and they may or may not be available as add on features. Then as systems and networks are interconnected IT has the challenge of protecting sensitive

network components from unsecured systems while establishing trust relationships between various domains and work groups sharing networked resources.

Monitoring tools for systems and management controls are expanding in availability and functionality but their use must be explicitly required for all sensitive systems if any degree of security, control and auditability is to be maintained. IT management too will be impacted by shifting emphasis in strategies for contingency planning and disaster recovery. Again backup and recovery tools may or may not be integral components of systems and networks, but the adequacy of any such techniques can only be assured in an environment where overall business recovery planning is integral to all system management and user responsibilities and recovery practices are regularly tested.

IMPACTS ON INTERNAL AUDITING MANAGEMENT

Auditors as users and reviewers of technology must maintain a keen awareness of new and increased areas of risks and the shifting control responsibilities and techniques.

Determining the Auditing Approach

For any organization this involves assessing ongoing business requirements and comparing them to short and long term automation strategies. Management's philosophy toward automation must also be taken into account when considering the appropriateness of plans, budgets, and stated objectives.

The IT organization structure and whether the organization employs a steering committee for automation resources will impact the expectable level of controls and auditability in the various systems areas subject to audit. The extent of deployment of user controlled systems and networks and the availability of centralized resources to authorize and/or support end user systems is also significant. The greater the extent of distributed activities and systems, the greater the need for a centralized control over the acquisition, deployment and ongoing control over system resources.

Factors to consider in planning the scope and extent of audit activities, and the specific audit expertise needed to accomplish audit objectives include:

- Hardware and software systems and platforms for business and production systems in use as well as systems in planning and development,
- Automation policies and standards, service level agreements, quality assurance, performance monitoring and results,
- Security and control requirements, control system structures, contingency planning, and disaster recovery.

Technical Auditing Resources

Determining the technical resources required for any audit engagement must take into account the professional responsibilities of auditors and the expectations of those served by the audit function. The IIA's "Model Curriculum of Information Systems Auditing" defines technical expertise for auditors at three different levels of technical involvement. Level one technical competence is the minimum level of technical knowledge expected for all auditors from entry level to the chief audit executive. A level one auditor should understand basic technology and system concepts and be able to understand the system components supporting any business activity subject to audit. All auditors should, for example, understand the difference between application systems and systems software and have a general understanding of which systems should contain general business and process controls. They should also be able to carry out routine audit tests using

automated tools as provided by technical support staff, and understand the purposes and results of such tests.

The ability to manage audits in an automated environment requires a degree of knowledge defined as level two in the Model Curriculum. Auditors in charge of audit projects should be able to assess operations and system structures and determine where the control points should be in such environments. Further, level two auditors should be able to conduct preliminary analyses and determine the types and extent of testing required for business application systems. They should then be able to evaluate test results and assess whether weaknesses or errors are based in the application, the network, supporting systems software, or other systems components, inappropriate system design features, improper use of system components, weaknesses in system and program change control, user or operator error, inadequate monitoring, or some other systemic cause; and to whom specific findings and recommendations should be addressed.

The level two auditor should know when to alert audit or business management of a finding based on its degree of seriousness and when to call for specialized audit support expertise to further investigate technical matters or to deploy specialized audit support tools. Level two auditors should be capable of passing the Certified Internal Auditor examination demonstrating their competence to perform audits with appropriate support in any given environment subject to auditing. The competent level two auditor understands overall business concerns and audit roles and responsibilities and how they are impacted by systems and changing technologies.

The ability to develop and conduct technical systems audits is typically the responsibility of auditors defined at level three in the Model Curriculum. Level three auditors may specialize in individual audit areas such as networks, operating systems, database management systems, or even major applications and will become intimately familiar with brand named components of systems and how individual system components interact with other components as in networks or the use of special security monitors for a particular operating system or communication environment. Level three auditors may or may not be capable of functioning at level two depending on whether they have broad business and auditing knowledge in addition to in depth technical knowledge.

Technical auditing resources include the tools used by auditors at all levels. Audit tools provide both localized and remote auditing capabilities. For example, the auditor's initial review of local area networks in an organization may reveal a standardized structure with central control including standard system components and features. In such an environment the auditor can then develop an audit tool that can be transmitted to any LAN server and run on a prescribed schedule with the results transmitted back to the auditor for review. While such a system will require specialized knowledge to develop, the time and money savings of eliminating auditor travel to each LAN site can be significant.

Other audit support tools should also be centrally controlled for an organization. Auditors should use standard tools for accessing data, routine and specialized analysis, spreadsheet and databases, word processing, communications and other productivity techniques.

Communication capabilities of auditors should be germane to the realm of their audit coverage. If auditors function within a local environment then local electronic mail should be sufficient - unless the organization makes use of global electronic communications, then the auditor should also use global communications tools both to support their efforts and for familiarity purposes. Similarly the mix of audit support tools should closely follow the types of tools used in all areas of the organization(s) subject to auditing.

Self assessment as an auditing tool should include assuring the self assessment tools used by management support auditability objectives. The auditor should be able to attest to the validity of self assessment as applied throughout the organization, particularly in those areas where self assessment is an integral component to proving compliance with laws and regulations.

Continuous control monitoring (CCM) and continuous process auditing systems (CPAS) as previously described in this paper and more fully addressed in a manuscript by Professor Miklos Vasarhelyi (currently unpublished) are the tools that will define future effectiveness of systems and processes subject to auditing. The audit application of CCM and CPAS tends to improve management acceptance of such tools and leads to the use of greater intelligence in interactive system monitoring and control procedures. Artificial intelligence in expert audit assistance systems will improve the auditor's ability to apply both local and remote auditing techniques. Ideally systems and networks in the future will have robust native security, controls, monitoring and auditing features. In such environments auditors will be challenged to validate the ongoing effectiveness of such features and to design continuous improvements to knowledge based intelligent audit systems.

Auditing Management Strategies

Auditing management strategies for any organizations will be based on both professional auditing standards and the expectations of those relying on the results of audits. Financial and compliance auditing continue to be premier areas of audit attention, but no longer constitute the clear majority of all auditing activity. The 1991 *SAC* reports documented the first research showing financial/compliance auditors as less than 50% of the population of internal auditors surveyed. As indicated in the previous section of this paper on technical auditing resources, even financial/compliance auditors have significant responsibilities to address technology and other areas of organizational impacts in their work.

Operational and functional auditing are also heavily impacted by new and emerging technologies as they provide the bases for business process reengineering and other organizational changes. An appraisal of the feasibility of combining two separate organizations or functions, for example, must address the compatibility of systems and system management philosophies for the two organizations and the estimated impacts of combining them.

Quality and environmental auditing have emerged as relevant areas in virtually all organizations. The competence of auditors in these areas is based on strengths in both auditing expertise and quality or environmental management matters. In many cases the level of technical knowledge required for these specialties is similar in depth to specialized knowledge required of IT auditors. Further, quality and environmental auditors should be expected to be competent in the use of IT auditing tools and to maintain other areas of technical competence as described above.

IT auditing in many audit organizations is still searching for an identity. Attempts to promote technical expertise in "nontechnical" auditors has lead to various approaches described as integrated auditing. In some cases technical auditors were assigned to support teams of nontechnical auditors. In other cases the IT auditing function was eliminated under the theory that all auditors would address technical issues during their routine audits. Both of these approaches have met with difficulty as technical auditors quickly lose their edge as they are removed from performing technical functions, and nontechnical auditors do not have the expertise needed to address controls in complex systems environments.

Audit Administration

Audit administration must take into consideration the availability and use of technology tools, the ongoing development of such tools, and the training of auditors in their use. Support tools as well as specific audit standards must be provided by audit management for: planning and scheduling, setting audit objectives, pre-audit work, conducting the audit, evaluating results, communication of audit results, maintaining audit archives and supporting databases, providing potentially global access to audit databases by traveling and remote audit staff members, and follow-up on audit recommendations. Specific responsibilities of professional auditors in meeting audit expectations are both the subject of using the right tools and maintaining specific competence in an ever expanding realm of knowledge areas.

Professional auditing organizations all over the world are addressing issues and standards relevant to technical auditing and the technical competence of auditors. The International Federation of Accountants (IFAC) recently formed an Information Technology Committee (ITC) specifically to address technology issues relevant to accountants and auditors worldwide. At the initial meeting of this committee representatives from seven countries representing fourteen different professional associations addressed an action plan to cover high priority technology issues in auditing and accountancy.

Professional auditors in internal auditing and public accounting are collectively addressing important issues in: defining the roles and responsibilities of auditors in relation to technology, addressing the technical competence and related credentials of audit professionals, continuing technical education requirements, use of technology tools, meeting expectations of the auditing profession in general and specifically in technology matters, defining the professional body of knowledge for auditors, technology standards and technology auditing standards, the availability of supportive information and communications for audit practitioners, and much more.

1994 SYSTEMS AUDITABILITY AND CONTROL REPORTS

Much of the information in this paper is based on research by The Institute of Internal Auditors Research Foundation and is covered in greater depth in the *SAC* reports. The 1994 updates to *SAC* include the following modules and individual chapters.

***SAC* Module 11 - Emerging Technologies**:
1. Executive Summary
2. Object Technology
3. Open Systems
4. Telecommunications
5. Mobile Systems
6. Information Security
7. Document Management
8. Multimedia
9. Intelligent Systems

***SAC* Module 13 - Advanced Technology Supplement**:
1. Executive Summary
2. Client/Server Architecture
3. Local Area Networks
4. Electronic Data Interchange
5. Business Process Reengineering
6. Outsourcing

7. Private Branch Exchanges
8. Electronic Mail

SUMMARY/CONCLUSION

The auditing profession is dealing with technology issues in a variety of ways. The level of technical knowledge needed by auditors is increasing constantly both for auditors in general and for technical audit specialists. Auditors too are working to address the concepts of security, control and auditability and how they can best be implemented by those responsible for the organizations, activities and systems subject to audits. A critical element in the future viability of professional auditing will be how the profession addresses questions of technical competence for auditors and the related impacts on the credibility of work performed by, and opinions expressed by auditors. Technology is not a new concern but the increasing rate of technological innovation is increasing the pressure on auditors to devote more attention to technology matters.

This paper was prepared by Charles H. Le Grand, Certified Internal Auditor. The observations and opinions expressed do not necessarily represent those of The Institute of Internal Auditors or The IIA Research Foundation. However, the content of this paper is generally based on and consistent with the research, educational and other materials prepared and released by The IIA over the past 20+ years as related to evolving issues in technology and the corresponding positions of the profession of internal auditing as expressed by and through The IIA. Comments, questions and rebuttals are invited. Please direct them to the director of technology at IIA headquarters.