

13. Industrial Bank of Washington (IBW)

TCBA served as subcontractor to a national accounting firm to perform the annual audit of IBW. In addition, on an earlier engagement, TCBA assisted IBW in assessing the continuing soundness of its commercial asset-based borrowers by performing audits of borrowers' accounts receivable and by reviewing their internal control structure and financial statements. Reports furnished to the bank for each borrower included recommendations for improving the borrower's operations and financial management systems.

E. INFORMATION TECHNOLOGY ASSURANCE & CONTROL GROUP

As corporations and governmental organizations rely more heavily on technology to provide timely, complete, and accurate financial information in order to make critical business decisions and to comply with governing laws and regulations, TCBA has responded to the need for increased information security by creating the Information Technology Assurance & Control Group (ITAC). ITAC is a cadre of IT auditors and IT security specialists with extensive experience in multiple systems and platforms: from mainframe systems to LANs, from Unix to MVS. This team specializes in technology risk and vulnerability assessments, IT audit techniques, and security assessments.

ITAC has significantly improved the service delivery process of TCBA and has clearly distinguished TCBA from its competitors. Through ITAC, TCBA provides superior services to existing and new clients through reviews and advisory services on emerging opportunities and threats relating to technology security.

Services

The ITAC group provides the following services:

- Electronic audit of financial transactions
- IT risk assessments
- Internet security and vulnerability testing
- Operating systems security reviews
- Logical and physical security reviews
- Network security assessments
- Perimeter protection and network reviews
- Database security
- Data integrity testing
- E-commerce/EDI reviews/Systrust/WebTrust
- IT regulatory compliance reviews
- System implementations evaluations
- General and application controls reviews
- Independent Verification and Validation (IV&V) services
- Business continuity planning and disaster recovery planning
- Security policy development and training
- Regulatory compliance with HIPAA, Sarbanes-Oxley Act, OMB Circulars, FISMA
- SAS 70 reviews, Gramm-Leach-Bliley Act
- IT strategic planning assistance
- Penetration testing
- System certifications and re-accreditation

Authorities and Regulatory Bodies

Most of our engagements are governed by or relate to reputable and industry accepted authorities and bodies.

- American Institute of Certified Public Accountants (AICPA)

- Information Systems Audit & Control Association (ISACA)
- International Information Systems Security Certification Consortium (ISC)
- Generally Accepted Systems Security Principles
- Rainbow Series - Minimum Security Requirements (MSR)
- NIST 5133
- British Standard (BS) 17799
- Internet Activities Board (IAB) Ethics and the Internet
- Computer Security Act 1987
- Privacy Act of 1974
- OMB Circulars A-123, A-127 & A-130
- FMFIA
- JFMIP

Selected ITAC engagements are summarized below:

1. District of Columbia Financial Audit

TCBA's ITAC group performed general and applications control reviews of the District of Columbia agencies during the annual audit for the Comprehensive Annual Financial Report. ITAC's general controls review of the District included the following areas:

- IT organization and management
- Access controls
- System software maintenance
- Service continuity
- Change control
- Local Area Network/Wide Area Network

The applications control review was an interactive effort with the financial statement auditors, where key IT-related controls were identified in the District's applica-

tions, and IT professionals tested the design and effectiveness of those controls.

2. Prince George's County Department of Housing and Community Development (DHCD)

The DHCD engaged TCBA to perform IV&V procedures for its new financial management system implementation. DHCD elected to close out fiscal year 2001 on the existing system (PHAMIS) and begin the new fiscal year using Emphasys. Emphasys was fully implemented in August 2001. DHCD's financial data maintained in PHAMIS was transferred through a combination of automated conversions and manual conversions. The transactions relating to Fiscal Year 2002 were posted directly to Emphasys.

The uniqueness of this engagement was that we had to perform the IV&V as a post mortem to the conversion process. The primary objectives of this engagement were to verify that financial data integrity was maintained throughout the conversion process and to verify that there were controls in place to ensure data and transaction integrity is maintained throughout the application. TCBA reviewed documentation including the conversion plans, issues logs, mapping and cross walk documents, security profiles, and other systems documentation. TCBA also developed test plans to test the conversion.

3. DC Water and Sewer Authority

TCBA's ITAC group performed a general and applications control review of this entity as part of the annual financial audit. ITAC's general controls review covered the following areas:

- IT organization and management
- Access controls
- System software maintenance
- Service continuity
- Change control
- Local Area Network/Wide Area Network

TCBA's ITAC Group also performed similar engagements for the DC Lottery and Charitable Games Control Board, Lincoln University, DC Department of Corrections, and United Planning Organization.

4. U.S. Pension Benefit Guaranty Corporation

TCBA is providing the PBGC with support services in compliance with the Federal Managers Financial Integrity Act (FMFIA). The services include internal controls support in the form of Independent Verification and Validation (IV&V) and Control Objectives Validation and Integration. The Control Objectives Validation process is designed to ensure that control objectives identified for PBGC's automated information systems are achieved through the application of automated operational, administrative, and management control techniques specifically designed for this purpose. This engagement includes the following tasks:

- Develop a plan for testing the automated and manual control techniques implemented over their main automated information system.
- Establish testing schedule and conduct the test of the control techniques.
- Review and analyze the test results to determine whether the control techniques employed are effective in meeting the control objectives.
- Document our observations and identify potential control weaknesses and mitigating controls and make recommendations for improvements to strengthen internal controls.

5. Control Objectives Identification and Integration for the Pension Benefit Guaranty Corporation

PBGC is in the process of improving the controls over its automated information system known as Participant Records Information Systems Management (PRISM). Federal regulations require that agencies ensure that government resources are used efficiently and effectively to achieve intended program results. This includes planning for and implementing adequate internal controls and security controls to minimize the potential for waste, fraud, and mismanagement. TCBA is conducting required Control Objectives Identification and Integration for PBGC's PRISM system. Our processes are designed to ensure that all systems used to pay benefits to participants comply with federal regulations. The tasks associated with this project are as follows:

- Identify the control objectives that are relevant to the development or major systems enhancement being contemplated.
- Evaluate the development team's plan to mitigate the threats and risks identified in task 1 and make appropriate recommendations for unmet control objectives.
- Review the system test plan to determine whether the control objectives identified in task 1 are adequately tested and make recommendations to modify the test plan to address the controls not considered.
- Provide support to the independent verification and validation (IV&V) team to ensure that the control techniques employed are effective in meeting the control objectives relevant to the system being developed and make recommendations for improving controls.

6. The District of Columbia HIPAA Compliance

TCBA's ITAC Group is playing a significant role on a contract to provide HIPAA compliance assessment and remediation to the District of Columbia's "covered entities." The primary responsibility of TCBA is to assist the HIPAA Project Management Offices (PMOs) of the various agencies achieve HIPAA compliance. Accordingly, TCBA performs gap analysis of the entity environment, provides remedial action plans, performs user awareness training, promotes public awareness through notices and brochures, and provides security and data safeguard advisory services. TCBA also provides guidelines on data safeguard standards, policies, procedures and practices and has provided HIPAA compliance services for the following agencies:

DC Department of Health (DOH)

TCBA's ITAC Group was assigned a leadership role in facilitating DOH's efforts toward HIPAA compliance. Throughout this effort, ITAC functioned as the defacto information security office responsible for HIPAA related security and data safeguard issues. Specific accomplishments include assisting in developing comprehensive policies and procedures and providing hands-on training to data center staff and the Chief Information Officer. ITAC also provided on-the-job training and structured classes for the designated information security officer.

DC Department of Mental Health (DMH)

TCBA's ITAC Group developed an IT auditing unit for the agency. This included assisting in developing an audit charter, developing an IT auditing handbook, an IT auditing policies and procedures manual and other auditing templates and tools. ITAC trained the

Information Security Officer in auditing and compliance review. ITAC performed compliance field audits of DMH units including the St. Elizabeth Hospital Center. Other similar HIPAA related tasks include remediation for the DC Department of Correction.

7. DC Government, Chief Technology Office

TCBA provides support to DC Office of the Chief Technology Officer (OCTO) Computer Security Management (OCSM) in the planning, implementation, and conduct of information systems security auditing to include developing information system security auditing standards; developing information system security auditing program plan; developing and implementing the audit methodology; identifying, evaluating, procuring and testing of information security system audit tools, conducting information security system audits; documenting procedures, processes, technical specifications, implementation plans, and configurations of daily tasks for the continuation of the auditing project; interacting with District employees, contractors and stakeholders to address matters concerning information system security audits; coordinating with OCTO and other agencies to evaluate and implement information system security auditing procedures and supporting the OCSM security architecture strategic program plan and OCTO enterprise architecture initiatives.