CITY OF SAN ANTONIO

INTERNAL AUDIT DEPARTMENT

Information Technology Services Department

Review of Authorized Remote Access to COSA Network

Project No. AU05-018

Release Date: August 30, 2005

Patricia Major CPA, CIA, CTP, CGFM
Frank Cortez CIA, CISA
Oscar Salazar

EXECUTIVE SUMMARY 1
Overview 1
Results In Brief 1
Background 1
Figure 1 – COSA Network 1
Figure 2 – High Level Review of Authorized Remote Access Points 1
Figure 3 – Remote Access Security Management 1
Figure 4 – Responsibility Matrix 1
Objective 1
Scope 1
Figure 5 – Authorized Remote Access Audit Scope 1
Criteria 1
Methodology 1
Conclusion 1
Figure 7 1
Table – Maturity Levels 1
Figure 8 – CobiT Maturity Model: DS5 – Ensure Systems Security 1
CONDITION STATEMENTS AND MANAGEMENT ACTION PLANS 1
Issue #1: Enterprise Security Strategy 1
Issue #2: Third-party Security and Confidentiality Agreements are not available 1
Issue #3: Remote Computer Security Tools 1
Issue #4: Remote Access Method (i.e., Dial-in, VPN, Citrix, Wireless/Modem-Air Cards) 1
Figure 9 – All Dial-In Users 1
Issue #5: Firewall and Intrusion Detection System Configuration 1

EXECUTIVE SUMMARY

Overview

The City of San Antonio's (City) information technology network provides online services for the public, employees, and domestic and international business relationships. Online services such as employment openings, electronic payments, bids, contract proposals, and requests for public information can be obtained through the City's website. Advances in networking technology have made remote access available through less expensive public communication facilities, such as the Internet and satellite technology. As more methods are authorized for remote access to the City's network, the complexity associated with protecting information increases. As a consequence, the potential for unauthorized access and harm increases, if security controls are inadequate.

"Authorized Remote Access" is the ability for a user, authorized by City Management, to connect and gain access to physically dispersed network resources. In general, remote access to the network may be achieved from any global site through the use of Internet connection, private network, dial-in modem, wireless, satellite and other technologies. This enables users to read e-mail, run applications, or transfer files between computers. This also allows computer technicians/programmers to troubleshoot incidents. While the benefits are highly recognized, detecting unauthorized remote access and inappropriate computer activity is an ongoing challenge for the Internet and network security teams.

A review of remote access methods to the City's network was conducted between February and May 2005. The review was designed to assess the Information Technology Services Department (ITSD) performance in managing the risks associated with "Authorized Remote Access". This review was based on employee interviews, process observations and documentation review.

Without adequate protection for remote access, significant risks of compromise exist, including data tampering, fraud, disruptions to critical operations, inappropriate disclosure of sensitive or private information and non-work related web surfing.

Results In Brief

Several concerns in need of attention related to improving ITSD remote access security controls were identified during the audit and are outlined below:

- Enterprise security strategy not available;
- Remote access security administration directives not complete and approved for distribution;
- Firewall and intrusion detection controls need improvement;
- Third-party security agreements do not exist; and
- The configuration, operation and management for remote access needs improvement

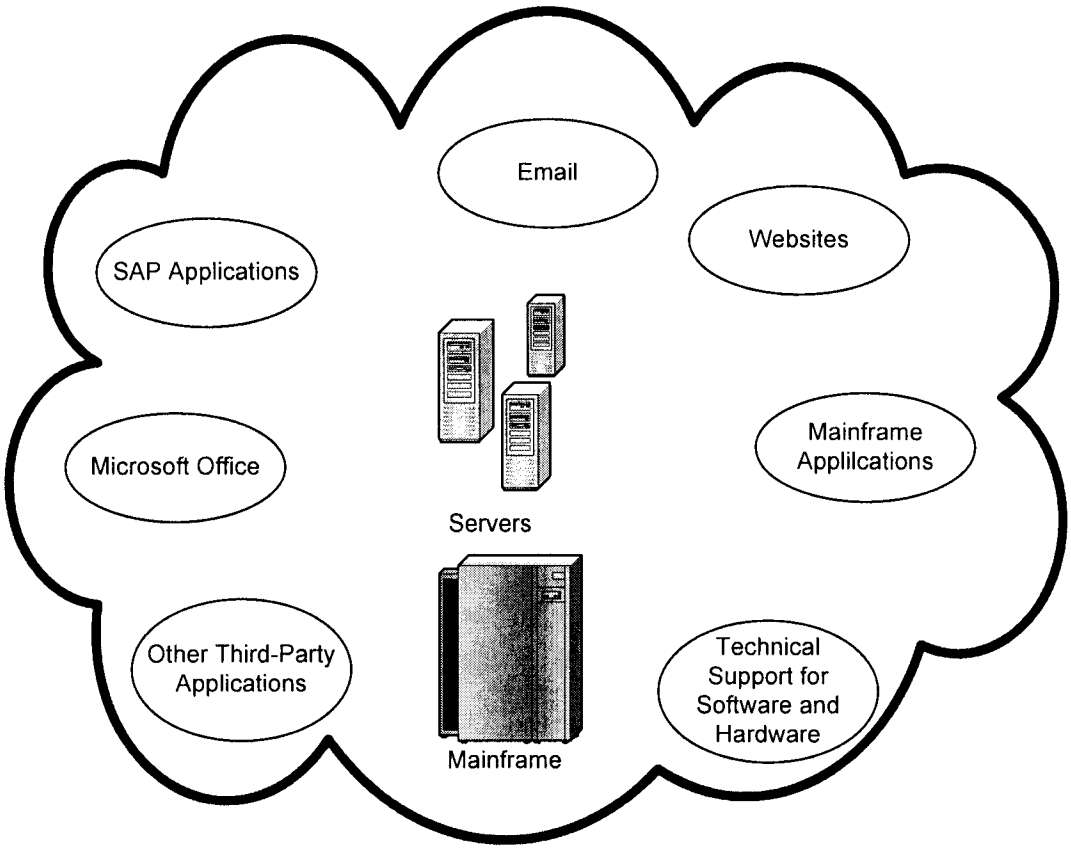
Improving security controls will help to establish acceptable levels of risk and rules covering such matters as employees dialing from home to the City network or granting third-party access to the network.

Background

ITSD manages remote access through various technology network methods and hardware and software devices. The primary reason for remote access is to allow employees and non-employee access from an outside entity such as a home or other remote destination. The purpose is to perform work or services for the City. Access is granted by approved request. City employees and non-city employees are granted access through work orders submitted by the City Department Data Security Administrator (DSA). An account ID is created and access is granted to specific applications and systems inside the COSA network such as electronic mail (E-mail), database applications, WEB and desktop applications, and technical and administration support for computer hardware and software as shown in **Figure 1**.

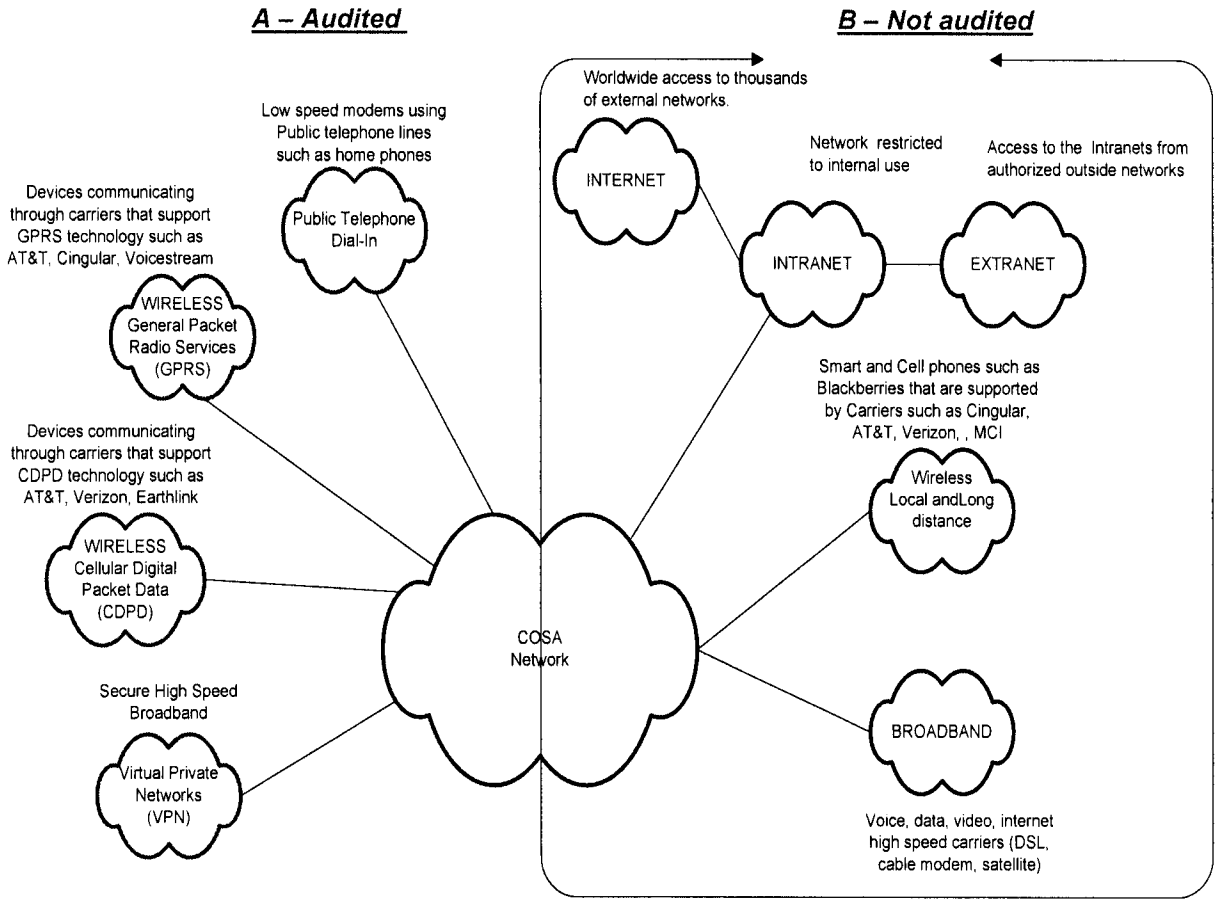
During the course of this audit, a new interim CIO hired by the City Manager, immediately led to a reorganization of ITSD personnel and responsibilities. It was not clear whether the new reorganization is aligning itself to meet security best practices.

Figure 1 – COSA Network



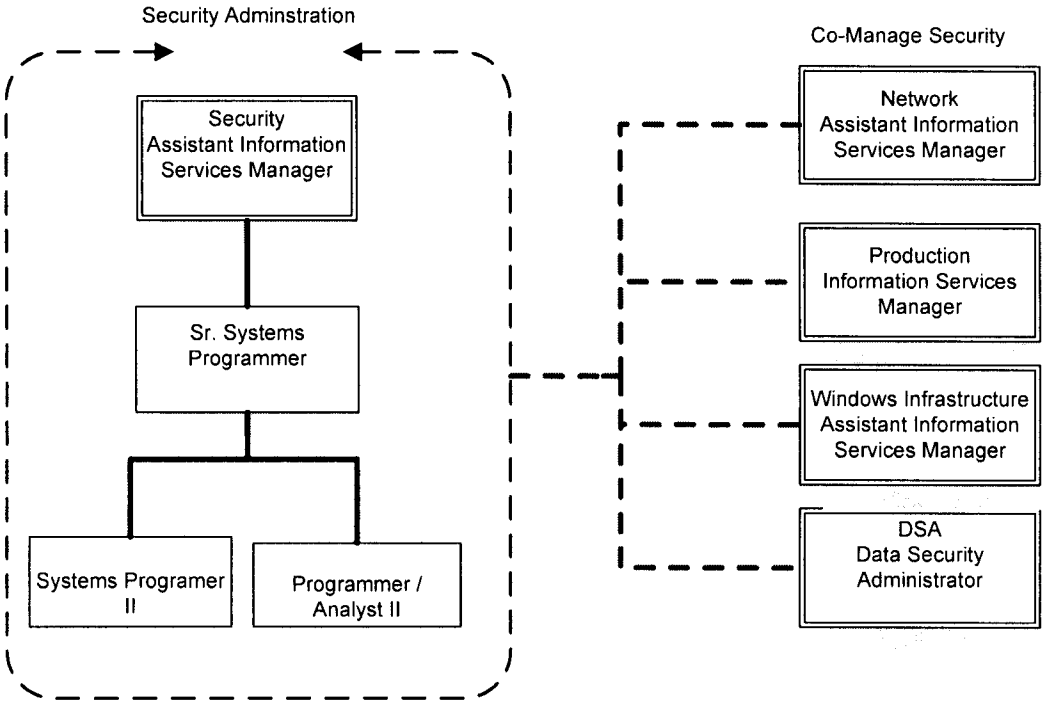
The methods and devices used to communicate with the City's network can vary depending on user requirements and needs. **Figure 2** illustrates the access methods included in the scope of this audit.

Figure 2 – High Level Review of Authorized Remote Access Points



There are three staff employees and one Assistant Information Services Manager supporting operations security at ITSD. Personnel in other department teams co-manage security with the Information Security Team as shown in **Figure 3.**

Figure 3 – Remote Access Security Management



Responsibilities for operations security, remote access configuration and support may involve one or more functions (**Figure 4**).

Figure 4 – Responsibility Matrix

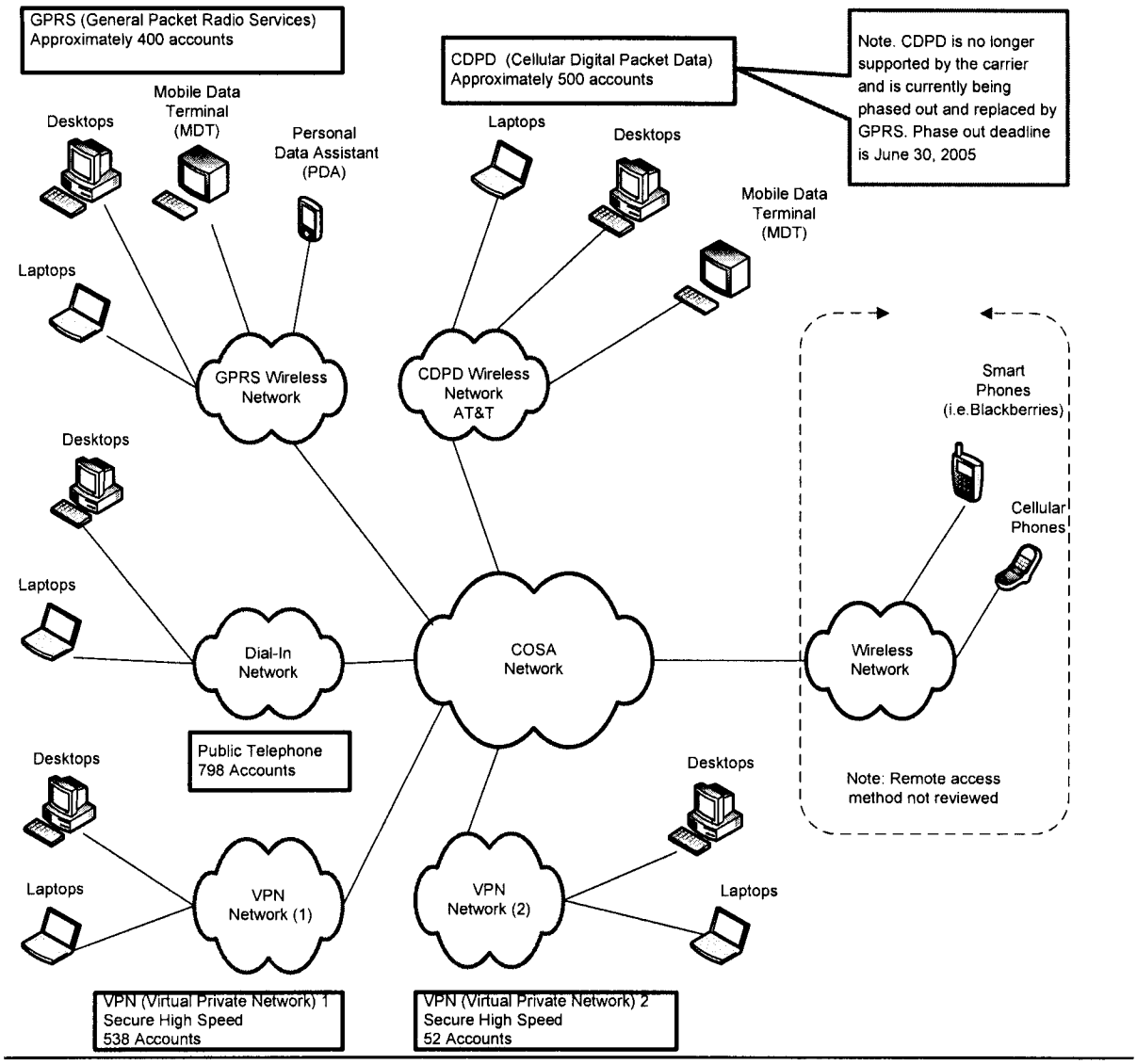
System	Functions
Dial-In	Security / Network
Virtual Private Network (1)	Security / Network
Virtual Private Network (2)	Security
Wireless	Network
Intrusion Detection System	Security
Firewall (1)	Security
Firewall (2)	Security
Long distance "Road Warrior" Dial-in Accounts	Network
Certificates	Security

Objective
The objective of this audit was to assess ITSD's performance in managing the risks associated with current technologies used for "Authorized Remote Access" to the City's network resources.

Scope
The scope of this audit was limited to "Authorized Remote Access" controlled by ITSD. The audit assessed high-level computer security access controls and directives for dial-in, wireless and virtual private network (VPN) remote access for telecommuting as shown in **Figure 5**. The audit covered the controls and directives that were in place as of May 1, 2005.

During our fieldwork, other ITSD priorities and commitments superseded audit team requests for timely documentation, data and personnel availability. Two requests were delayed by three weeks and one received no response at all. The requested items were finally delivered after the close of field work, thus limiting audit team review of wireless access methods.

Figure 5 – Authorized Remote Access Audit Scope



Criteria

To measure performance, audit staff used criteria based on City directives and procedures, Control Objectives for Information and related Technology (CobiT) and best practices.

The IT Governance Institute (www.itgi.org) developed CobiT as an open standard using non-technical language to help focus information technology in support of overall business goals. CobiT was selected as the criteria for measurement because it addresses business objectives and is easy to understand. CobiT continues to gain acceptance internationally and is evolving due to support from the IT Governance Institute.

In addition to standards such as CobiT, there are other industries based or technology specific guidelines that can be used to measure the effectiveness of an organization's controls. The Center for Internet Security (CIS) and SANS (SysAdmin, Audit, Network, Security) Institute both provide baselines to be used for enhancing controls at more detailed levels.

Methodology

The review was performed in compliance with generally accepted government auditing standards (GAGAS) issued by the U.S. Government Accountability Office (GAO) and other criteria to conform with the Institute of Internal Auditors' "International Standards for the Professional Practice of Internal Auditing."

Government Auditing Standards requires a peer review of auditing practices at least once every three years by reviewers independent of the audit organization. The City Internal Audit Department (CIAD) had its last external peer review in July 2001. CIAD is scheduled for the next peer review in August 2005.

Audit staff used the following techniques in this engagement:

- Reviewed directives and procedures provided by ITSD;
- Performed inquiries with ITSD employees;
- Reviewed process maps (or flow charts) used by ITSD staff;
- Conducted an analysis of the controls in place to safeguard against unauthorized access; and
- Selected sample access requests from the Logon Identification System (LIDS) to verify authorized users.

Conclusion

After the completion of audit procedures, a conclusion was made on the effectiveness of access controls for "Authorized Remote Access". The conclusion was based on characteristics of the CobiT control objective maturity model for DS5 – Ensure Systems Security capabilities. Further description of the capability stages has been included as **Figure 8**.

The maturity models represent a method of scoring so that an organization can measure itself from "nonexistent" to "optimized" using best practices in controlling IT security. The premise of maturity measurement is that an organization can move to the "optimized" stage by meeting all conditions described for this level. Auditing and Management can both use this tool to self-assess or reference the conclusion of independent review shown in **Figure 7.**

Figure 7

Table – Maturity Levels

0 - Non-existent	Management processes are not applied at all
1 – Initial	Processes are "Ad Hoc" and disorganized
2 - Repeatable	Processes follow a regular pattern
3 - Defined	Processes are documented and communicated
4- Managed	Processes are monitored and measured
5 - Optimized	Best practices are followed and automated

At the completion of this review, it was determined that the capability stage for managing "Authorized Remote Access" risks and control responses was "**Repeatable**". This defines the current position of the City's maturity relative to IT control and governance maturity.

The most recent industry trends survey for the maturity levels of CobiT was conducted in 2002; final closure of this survey was June 2002. At the end of the survey, the findings revealed the average maturity levels by industry type as shown below.

Finance	3.0 - Defined
Public Sector	2.0 - Repeatable
Retail & MFG	1.5 - Repeatable

*Source: *ISACA Information Systems Control Journal, Volume 6, 2002*

As of 2005, the City of San Antonio remains level at the "Repeatable" stage. New government regulations such as Sarbanes Oxley and HIPPA require compliance over financial and critical organization data. This requires stricter security controls to adhere with compliance. At this stage the City Manager and Council should support ITSD efforts to evaluate and develop a strategy for improvement.

Figure 8 – CobiT Maturity Model: DS5 – Ensure Systems Security

Stage	Procedures
Non-existent	• The organization does not recognize the need for IT Security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no IT security reporting and no response process to IT security breaches. There is a complete lack of a recognizable system security administration process.
Initial	• The organization recognizes the need for IT security, but security awareness depends on the individual. IT security is addressed on a reactive basis and not measured. IT security breaches invoke finger pointing responses if detected, because responsibilities are unclear. Responses to IT security breaches are unpredictable.
Repeatable	• **Responsibilities and accountabilities for IT security are assigned to an IT security coordinator with no management authority. Security awareness is fragmented and limited. IT security information is generated, but not analyzed. Security solutions tend to respond reactively to IT security incidents, and adopt third-party offerings, without addressing the specific needs of the organization. Security policies are being developed, but inadequate skills and tools are still being used. IT security reporting is incomplete, misleading or not pertinent.**
Defined	• Security awareness exists and is promoted by management. Security awareness briefings have been standardized and formalized. IT security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for IT security are assigned, but not consistently enforced. An IT security plan exists, driving risk analysis and security solutions. IT security reporting is IT-focused, rather than business-focused. Ad hoc intrusion testing is performed.
Managed	• Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Security policies and practices are completed with specific security baselines. Security awareness briefings have become mandatory. User identification, authentication and authorization are being standardized. Security certification of staff is being established. Intrusion testing is a standard and formalized process, leading to improvements. Cost/benefit analysis, supporting the implementation of security measures, is increasingly being utilized. IT security processes are coordinated with the overall organization security function. IT security reporting is linked to business objectives.
Optimized	• IT security is a joint responsibility of business and IT management, and is integrated with corporate security business objectives. IT security requirements are clearly defined, optimized and included in a verified security plan. Security functions are integrated with applications at the design stage, and end users are increasingly accountable for managing security. IT security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed with formalized incident response procedures supported by automated tools. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk are the basis for continuous improvements. Security processes and technologies are integrated organization wide.

*Source: IT Governance Institute, "*Control Objectives for Information and Related Technology*" (CobiT)

CONDITION STATEMENTS AND MANAGEMENT ACTION PLANS

The following observations, recommendations and management responses were recorded as a result of work procedures performed. They are presented in order of significance.

Issue #1: Enterprise Security Strategy

Condition
An enterprise security strategy and plan for protecting the City's information assets is non-existent. It was repeatedly stated by the security manager that security responsibilities are unclear for the assurance of safeguarding the City's data. This has resulted in risk management for remote access technology not being guided by any formal management directives. Administrative Directives related to remote access security have been in draft form since January, 2003. They have not been approved for content, or promoted for distribution to all users. Additionally, these draft Administrative Directives (ADs) do not address new methods of dial-in and virtual private network remote access, or non-standard remote access software such as 'GOTOMYPC'.

Administrative Directive 7.3, "Responsibilities", states that "the Information Resources Department shall be responsible for developing, maintaining, publishing and administering a comprehensive Data Security Plan. This plan shall reference applicable statutes, ordinances and Administrative Directives pertaining to Data Security."

Criteria
CobiT Control Objective AI4 - Developing and Maintaining Procedures specifies that to ensure the proper use of the applications and the technological solutions put in place, operational and user procedures and controls should be enabled.

Administrative *Directive 7.3 Data Security Policies and Procedures,* effective January 1, 1990 establishes policy and responsibility for ensuring the security, privacy, and confidentiality of data maintained by City departments in computerized systems.

Administrative Directive 1.1 General Provisions, effective June 25, 1980, outlines the procedures for the implementation, responsibility and format of ADs. It states that the "City Manager will review and approve all ADs prior to their implementation."

Cause
The ITSD Security Team has not been able to obtain City Executive Management approval for draft Computer Security Remote Access ADs.

Effect
Adverse consequences of inappropriate or unauthorized use of remote access technology increase without defined and published management expectations for proper computer and network use. Some consequences include: (1) Virus infections causing denial of service and work stoppages; and (2) User account and password compromise can result in information theft and disclosure of private information.

Recommendation
An enterprise security strategy should be developed that includes controls for:

- Confidentiality, integrity and availability of data ; and
- Clear roles and responsibilities for managing security risks.

The Chief Information Officer should submit draft Computer Security Remote Access ADs to the City Manager for approval. Once approved, these ADs will help define management's expectations for proper computer and network use and management of information security risks.

Computer Security Remote Access ADs would help minimize security risks by:

- Providing guidelines for user acceptable use of computer resources;
- Promoting a consensus and better understanding of information technology security objectives for City business operations;
- Ensuring the greatest information technology security risks to City's business operations are identified and addressed on an ongoing basis;
- Establishing a foundation for supporting information technology security directives designed to address technology risks in specific areas (e.g. e-commerce, Internet access, SAP application security, network security, encryption of business documents, e-mail usage, and classification of information assets);
- Clearly defining responsibilities for computer security administration; and
- Promoting development and communication of information and technology standards to acquire, manage, and use information technology effectively to protect investments.

Management Response

The Strategic Initiatives Division of ITSD will develop an enterprise security strategy that includes controls for confidentiality, integrity, and availability. The security strategy should encompass the ten security domains as outlined by the International Information Systems Security Certification Consortium (ISC)[2].

I. Access Control Systems and Methodology
II. Applications and Systems Development
III. Business Continuity Planning
IV. Cryptography
V. Law, Investigation and Ethics
VI. Operations Security
VII. Physical Security
VIII. Security Architecture and Models
IX. Security Management Practices
X. Telecommunications, Network and Internet Security

Previously a remote access policy had been drafted but it had never been submitted to the City Manager for consideration as an administrative directive (AD). A Remote Access policy will be developed and submitted as an administrative directive (AD) to the City Managers Office.

Responsible Party for Implementation

Strategic Initiatives Division

Implementation Date: October 31, 2005.

Issue #2: Third-party Security and Confidentiality Agreements are not available

Condition
The ITSD Security Team was not aware of any binding agreements between the City and third-parties that have been authorized to provide technology support remotely for City computer systems. This includes entities such as SAP, Hansen Information Technologies, Open Systems Group, and other business and professional services. Third-party agreements are a key component to protecting the integrity and confidentiality of City owned data.

Criteria
CobiT Control Objective DS2 - Managing Third-Party Services specifies that control measures be implemented to ensure that roles and responsibilities of third parties are clearly defined, adhered to and continue to satisfy requirements.

Cause
The ITSD Security Team has not been able to obtain City Executive Management approval to third-party and extranet draft security directives and agreements.

Effect
The City's vital computer operations could potentially be disrupted by ineffective third-party controls which result in viruses penetrating the COSA network or confidential data being disclosed.

Recommendation
The Chief Information Officer should submit draft third-party agreements to the City Manager for approval. Once approved, third party agreements will define management's expectations for proper computer and network use and management of information security risks. Third-Party agreements would help minimize security risks by including, at a minimum, the following:

- Definition of the nature of the agreement and the conditions under which City data can be viewed and used; and
- Definition of a confidentiality agreement between the third-party and its employees to provide additional protection from disclosure or abuse of City information.

Management Response
A standard third-party agreement should be a part of all contractual agreements with third-parties that are entered into by the City. The Strategic Initiatives Division of ITSD will draft a third-party agreement that define the specific details to define the conditions in which City Data can be viewed and used and provide a mechanism to protect the City from disclosure of information on the part of the third-party.

Responsible Party for Implementation
Strategic Initiatives Division

Implementation Date: October 31, 2005

Issue #3: Remote Computer Security Tools

Condition
Administrative directives addressing anti-virus and other security tools have not been approved and distributed to City employees and third-parties using non-city owned computers to connect to the City's network. Minimum required security tools should include the use of current anti-virus and personal firewall software.

Criteria
CobiT Control Objective DS5 - Ensuring Systems Security specifies that information should be safeguarded against unauthorized use, disclosure or modification, damage or loss by restricting access to authorized users taking into consideration controls including virus prevention and detection, firewalls and tools for monitoring compliance.

Cause
The ITSD Security Team has not been able to obtain City executive management approval for draft Antivirus and Firewall Administrative Directives.

Effect
The risk of disruptions to critical operations and disclosure of sensitive or private information increases if personal firewalls and up-to-date anti-virus software is not required for all computers allowed remote access to the COSA network.

Recommendation
The Chief Information Officer should submit the Antivirus and Firewall draft Administrative Directive to the City Manager for approval. The approved ADs define management's expectations for appropriate computer and network use and management of security risks associated with remote computers.

It is also recommended that a process be implemented for monitoring compliance.

Management Response
The draft remote access administrative directive should dictate that no remote access to the City's network will be permitted if the client does not have approved anti-virus and anti-firewall software installed on their computer.

ITSD has purchased a software package that provides an anti-virus and personal firewall that can be used to provide the enhanced protection that are required to meet the requirements for this issue. It is recommended that all city employees and third-parties connecting to our network be required to install this software. The use of this software will allow ITSD to centrally manage and control the anti-virus and personal firewall settings for all remote clients accessing the city's network remotely.

Responsible Party for Implementation
Policy: Strategic Initiatives Division and Chief Information Officer
Software: Chief Technology Officer

Implementation Date: November 2005

Issue #4: Remote Access Method (i.e., Dial-in, VPN, Citrix, Wireless/Modem-Air Cards) Internal Controls

Condition

A review of the remote access methods and associated internal controls revealed the following conditions:

1) Risk management processes and procedures have not been formally approved that address appropriate and required control measures based for each method of remote access.

2) Remote computer access controls can be circumvented by users dialing-in to the City's computer network using dial-in or wireless modems. This is because the access point for dial-in and wireless modem connection is behind the City's computer network firewall, thus bypassing standard remote access safeguards.

3) There is no administrative directive for authorized use of dial-in modems for the purpose of Internet surfing. The average monthly cost for both local and 1-800 dial-in is $4,657 or $55,885 annually.

4) Requests submitted for remote access are loosely monitored for unauthorized and suspect user accounts. A review of the authorized dial-in user list revealed questionable authorized access by some departments and users such the Open Systems Group consultant and the previous City Manager, (**Figure 9**). In addition, these questionable user accounts can be compromised allowing harmful activity if removal is not done in a timely manner.

5) Well defined directives for requesting remote access are not in place. It is unclear if ITSD directives and security best practices are being consistently followed by all DSAs. DSA's are responsible for submitting remote access requests for processing to the security teams. Training manuals are outdated and the trainers have been recently assigned to other departments leaving this function open.

Figure 9 – All Dial-In Users

Department	Users with Dial-in Access	
Alamo Dome	3	
Asset Management	1	
Aviation	4	
Budget	5	
City Attorney	6	
City Auditor	1	
City Clerk	1	
City Council	13	
City Council Act Team	4	
City Council District 10	1	
City Council District 1	3	
City Council District 2	6	
City Council District 3	3	
City Council District 4	4	
City Council District 5	6	
City Council District 6	1	
City Council District 7	1	
City Council District 8	3	
City Council District 9	1	
City Council Support	2	
City Manager	4	
City Manager Assistant	3	
City Manager Office	1	
Code Compliance	4	
Computer Solutions	3	
Contract Services	1	
Convention Facilities	2	
Cultural Affairs	2	
Customer Service - 311	5	
Convention Visitors Bureau	28	
Community Initiatives	52	
Development Services	15	
Economic Development	9	
Environmental Services	2	
Enterprise Resource Management	2	
External Relations	1	
Finance	8	
Fire	21	
Generic accounting backup	**1**	*
Housing & Community Development	2	
Isabel Gonzaba Global Scape (IG Consulting)	**2**	*
Internal Affairs	3	
Radio Communications Contract Consultant	**1**	*
Information Technology Services Department	**118**	*
Library	10	
Neighborhood Action	5	
Open Systems Group Consultant	**1**	*
Parks & Recreation	17	
Performance Analysis Team	1	
Public Utilities Office	2	
Public Works	12	
Purchasing	2	
Metro Health District	23	
Police	19	
Information Technology Services Department (IT Security)	2	
Total	**453**	

*Note: Requires immediate attention for accuracy

Criteria
CobiT Control Objective DS5 - Ensuring Systems Security specifies that information should be safeguarded against unauthorized use, disclosure or modification, damage or loss by restricting access to authorized users taking into consideration controls including virus prevention and detection, firewalls and tools for monitoring compliance.

Cause
ITSD has not implemented well defined administrative controls for remote access methods.

Effect
The risk of viruses infecting the City network increases when users use dial-in and wireless connections with proper controls in place. Users have the ability to download virus infected software, illegal movies or music, or abuse internet privileges by surfing the Internet.

Recommendation
ITSD should improve the configuration, operation and management of remote access methods by:

1. Requesting that Executive Management review and approve risk management processes and procedures;
2. Evaluating firewall protection measures for modem users;
3. Submitting a directive for authorized modem usage and acceptable Internet use during remote dial-in access to the City Manager for approval;
4. Obtaining a war-dialer so potential unauthorized modems can be detected;
5. Evaluating charge back costs to each department using modem dial-in (local and long distance numbers) to manage risks;
6. Immediately removing suspect/recognized user accounts; and
7. Establishing benchmarks and measures for DSA's that represent best practices for improvements in the areas of training, technical knowledge, empowerment and devotion to comply with ITSD directives.

Management Response
Management concurs with action items addressed below:

1. Develop formal risk management procedures and submit to executive management for review
2. Remote Access users should be moved to a network segment behind a firewall to provide enhanced protection.
3. The acceptable use policy administrative directive should encompass and be sufficient to cover remote access use.
4. Purchase a war dialer to identify, monitor and remove rogue modem devices.
5. A cost recovery for dial-in access will be developed to provide cost recovery and serve as an additional management control.
6. Quarterly audits on all remote access accounts will be conducted to ensure that all accounts are authorized and valid.
7. Establish standards for the Departmental Security Administration (DSA).

Responsible Party for Implementation

1. Quality Assurance office.
2. Network Security team.
3. The Strategic Initiatives Division of ITSD.
4. Network security team.
5. ITSD planning and administration
6. Network security team.
7. Network security team.

Implementation Date: December 2005

Issue #5: Firewall and Intrusion Detection System Configuration

Condition

The audit of ITSD's configuration of two computer network firewalls and one intrusion detection system revealed the following areas of concern:

- One of the two computer network firewalls is not fault tolerant. Fault tolerant means that the firewall is able to continue to operate following failure of a computer or network component. This could cause immediate interruption of remote access service.
- One of the two computer network firewalls creates an audit log which is not captured and stored in a different and secure media device for retrieval. Audit logs capture access information for authorized and unauthorized access.
- Only limited functionality for the intrusion detection system has been implemented. For example the software used is shareware and not the full commercial product. An intrusion detection system identifies unauthorized access.
- Firewall and intrusion detection system configuration procedures have not been approved and distributed.

Criteria

CobiT Control Objective DS5 - Ensuring Systems Security specifies that information should be safeguarded against unauthorized use, disclosure or modification, damage or loss by restricting access to authorized users taking into consideration controls including virus prevention and detection, firewalls and tools for monitoring compliance.

Cause

Firewall standards and procedures are not in place. A project to include fault tolerance, improve intrusion detection system functionality, and thus protect and store firewall logs has not been initiated.

Effect

The risk of security breaches increases due to the lack of a documented firewall security configuration baseline for the test and production computer network firewall and intrusion detection systems.

Recommendation

ITSD should improve the configuration, operation and management of its computer network firewall and intrusion detection systems by implementing the following:

1. Initiating and approving an appropriate fault tolerance configuration for firewalls. Include firewall standards that address best practices for:
   - Architecting and designing of firewalls;
   - Installing hardware and software;
   - Configuring network routing, logging and alerting;
   - Performing firewall testing;
   - Conducting internal and external penetration testing and testing frequency; and
   - Protecting and storing firewall logs for investigations

2. Initiating a project to review the design, architecture and effectiveness of the existing computer network intrusion detection system. Include Standards that address at a minimum:
   - Preventing intrusions;
   - Monitoring and reporting; and
   - Recovering

3. Developing a formal computer incident response team.
4. Approving an outside independent party to conduct penetration testing annually.

Management Response

The computer firewall which is not fault-tolerant will be migrated to the newer fault-tolerant firewall. The new firewall configuration will consist of four zones:

a) Demilitarized Zone
b) Secured Server Zone
c) Trusted Computer Zone
d) 'Untrusted' Computer Zone

1. Each zone will have a separate firewall rule base that provides adequate protection for each zone from the other zones.
2. All remote access will be moved to the 'untrusted' computer zone to include: GPRS, VPN, and Dial-In clients.
3. Remote access via the Citrix environment is controlled and provides secure remote access.
4. The firewall logs for the firewall are backed up and maintained for a period of 90 days.
5. ITSD will be establishing a formal incident response team that will include key members of the different IT divisions. The team will then establish incident response tactics and guidelines.

ITSD has deployed an open-source intrusion detection system widely deployed in many large enterprises and provides a robust intrusion detection engine. The intrusion detection system is still in its infancy and additional training and configuration is required. We will be looking into larger scaled enterprise intrusion detection systems/intrusion prevention systems at the beginning of fiscal year 2006.

Additionally, ITSD will be arranging an annual third-party evaluation of our entire security framework.

Responsible Party for Implementation

Network Security

Implementation Date: January 2006