THIS PUBLICATION CONSISTS OF TWO SECTIONS:

A) REPORT
B) APPENDIX

INFORMATION SECURITY METRICS
AN AUDIT-BASED APPROACH

This document describes an approach to measuring the effectiveness of information systems security activities within an IT organization. The approach incorporates industry standard control objectives and industry best practices in meeting these objectives. This approach allows an IT organization and/or an independent testing organization to measure security effectiveness while formally taking into account an information systems organization's unique control framework.

Key to measuring information systems security effectiveness is a clear statement of the objectives of information security controls. Adept information systems management organizations are able to demonstrate a systems control framework that corresponds to industry standard control objectives. Security is effective if management has achieved the control objectives that have been decided to be integral to its systems control framework.

That is, to demonstrate and measure system security effectiveness, there must be clear goals and objectives. An organization must assess risks in the

EXAMPLE ENVIRONMENT

An information systems organization decides that a given environment will be adequately secured if they follow these twelve industry standard control objectives: [1]

1. Manage Security Measures
2. Identification, Authentication and Access
3. Security of Online Access to Data
4. User Account Management
5. Management Review of User Accounts
6. User Control of User Accounts
7. Security Surveillance
8. Data Classification
9. Central Identification and Access Rights Management
10. Violation and Security Activity Reports
11. Incident Handling
12. Firewall Architectures and Connections with Public Networks

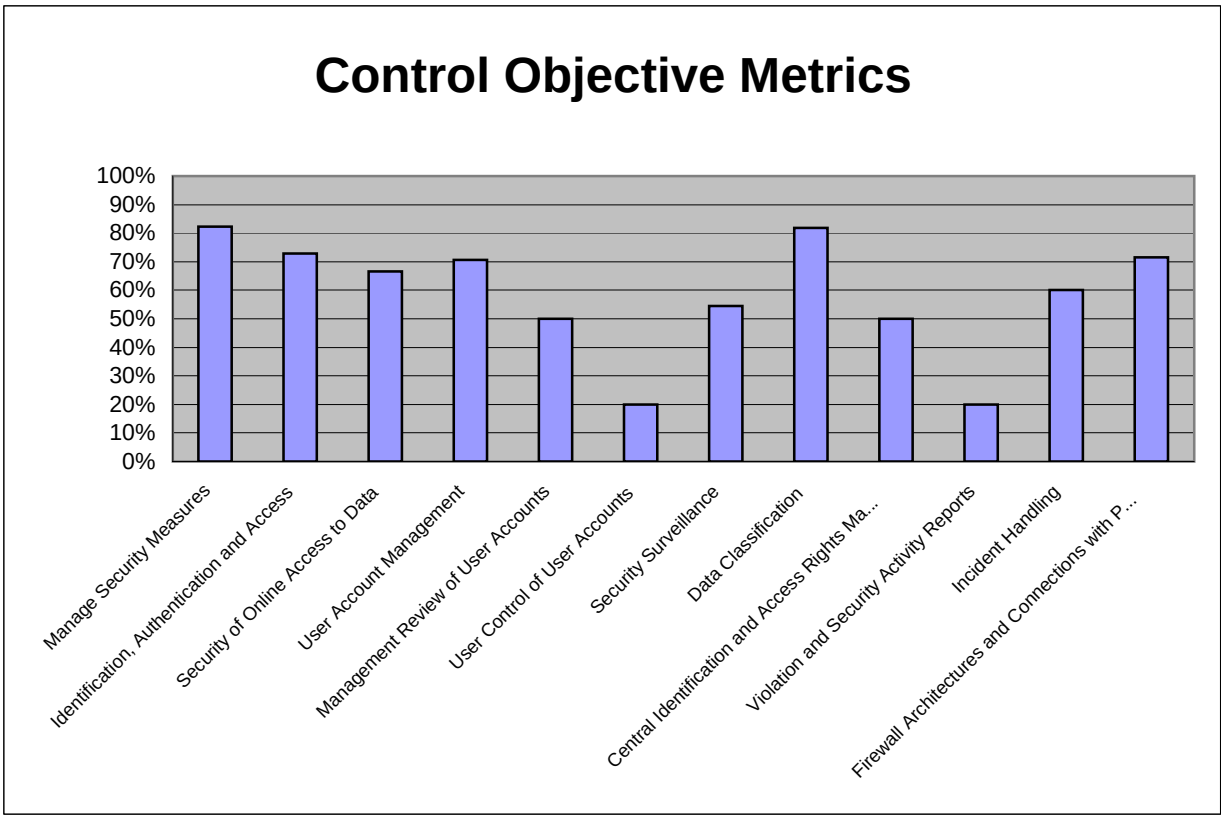
Having decided on these objectives, the organization creates its own systems control framework. It divides its information systems security activities into six processes:

1. Policy - to dictate organizational standards with respect to information systems security.
2. Awareness - to provide accountability.
3. Implementation - to address how policy is to be enforced.
4. Monitoring - to detect policy violations.
5. Compliance - to ensure policy violations are corrected.
6. Strategy - to align information systems security efforts to organizational goals.

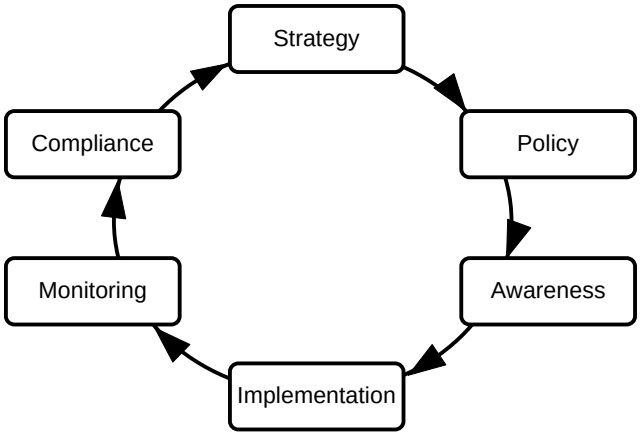
[1] The industry standard objectives are taken from the Control Objectives for Information and Related Technology Framework (COBIT), issued by the Information Systems Audit and Control Association (ISACA), 1998.

Appendix C

		#STEPS	Steps where test passed	%PASSED	Steps where test not passed	% NOT PASSED
1	Manage Security Measures	17	14	82%	3	18%
2	Identification, Authentication and Access	37	27	73%	10	27%
3	Security of Online Access to Data	3	2	67%	1	33%
4	User Account Management	17	12	71%	5	29%
5	Management Review of User Accounts	4	2	50%	3	75%
6	User Control of User Accounts	5	1	20%	3	60%
7	Security Surveillance	22	12	55%	10	45%
8	Data Classification	11	9	82%	2	18%
9	Central Identification and Access Rights Management	4	2	50%	2	50%
10	Violation and Security Activity Reports	5	1	20%	4	80%
11	Incident Handling	5	3	60%	2	40%
12	Firewall Architectures and Connections with Public Networks	7	5	71%	2	29%



The logical flow between these processes is depicted in the following diagram:[1]



Together, these processes comprise the organization's Systems Security Control Framework.

MEASURING SECURITY

Industry standard control objectives have a standard unit of measure in the Information Systems Audit. Audit steps specify the actions that an auditor would take to independently gather evidence of activity established by management that contributes to control objectives. But measuring control objectives does not need to be done by an external auditor, it could be done by an information systems security organization as part of its own monitoring process. Appendix A lists the control objectives adopted in the above example and sample audit steps that would traditionally measure whether the objectives are met. The final two columns in the table of Appendix A show how someone who is measuring the evidence contributing to a control objective could map that same activity onto an IT organization's Systems Security Control Framework. This type of worksheet provides assurance that an organization has provided resources adequate for achieving its own control objectives.

Where the execution of audit steps does not provide assurance that a control objective has been met, an auditor will seek a demonstration that management has established alternative controls that meet the objective. These activities are referred to as "compensating controls." This allowance for deviations in the measurement process should be critically examined, but it does allow the use of a standard audit program across organizations that may have very different ways of achieving the same control objective.

The completed information systems security measurements in Appendix A produce two sets of metrics (see Appendices C and D). The first will identify the control objectives that were successfully met. The second will identify the information security processes where improvements should be made in the control framework.

[1] Bayuk, J., *Security Through Process Management*, 19th Annual National Information Systems Security Conference, Baltimore, MD

Because the metrics compare industry standard objectives, they make it possible to compare the security environments at two different organizations. Because they use management's own selection of control objectives and allow for compensating controls, they should present a fair comparison even if the compared organizations have slightly different control objectives. These metrics may also be used for time-based comparisons within a single organization. As improvements are incorporated into the systems control framework, repeat measurements should demonstrate steady improvement over time.

APPENDIX A

	The plan is to test these control objectives:	which are characterized as:	and will be evident through executing the audit steps, which have been tailored to the environment under review:	Pass ? (Y/N)	Framework Component Pass=Y => existing Pass=N => suggested
1.1	Manage Security Measures	Information Technology security should be managed such that security measures are in line with business requirements. This includes: translating risk assessment information to information technology security plans; implementing of the information technology security plan; updating the information technology security plan to reflect changes in the information technology configuration; assessing the impact of change requests on information technology security; monitoring the implementation of the information technology security plan; and aligning information technology security procedures to other policies and procedures.	Obtain a copy of information security policy.	*Y*	*Policy*
1.2			Verify that the security policy production process identifies and addresses IT risks.	*Y*	*Policy*
1.3			Verify that the security policy production process identifies and addresses regulatory requirements.	*Y*	*Policy*
1.4			Verify that the security policy production process identifies and addresses management information needs.	*N*	*Policy*
1.5			Verify that IT requirements with respect to security measures follow policy.	*Y*	*Awareness*
1.6			Verify that security planning is integrated into the IT planning process.	*Y*	*Strategy*
1.7			Verify that the security implementation process identifies and addresses operational considerations.	*Y*	*Implementation*
1.8			Verify that decisions with respect to security mechanisms utilize accurate technology assessments.	*Y*	*Implementation*
1.9			Verify that procedures for access control and user authorization complies with policy.	*Y*	*Implementation*
1.10			Obtain evidence that procedures for access control and user authorization are followed.	*Y*	*Monitoring*
1.11			Verify that there is an IT security plan implemented for each system with the scope of the review.	*Y*	*Implementation*

APPENDIX A

1.12			Sample recent public security alert bulletins for the technology under review to assess the effectiveness of procedures by which security fixes are incorporated into the technology environment.	*N*	*Implementation*
1.13			Obtain evidence that security impact of changes is assessed in the infrastructure planning process.	*Y*	*Strategy*
1.14			Determine whether security measures are kept up to date with system infrastructure changes.	*Y*	*Implementation*
1.15			Obtain a copy of procedures for security monitoring.	*N*	*Monitoring*
1.16			Obtain a copy of information system procedures for operating system security configuration.	*Y*	*Implementation*
1.17			Determine whether security procedures are consistent with security policy.	*Y*	*Awareness*
2.1	Identification, Authentication and Access	The logical access to and use of the information services function's computing resources should be restricted by the implementation of an adequate authentication mechanism of identified users and resources associated with access rules. Such mechanisms should prevent unauthorized personnel, dial-up connections and other system (network) entry ports from accessing computer resources and minimize the need for authorized users to use multiple sign-ons. Procedures should also be in place to keep authentication	Obtain identification, authentication, and access granting procedures for the UNIX environment.	*Y*	*Implementation*
2.2			Obtain identification, authentication, and access granting procedures for the NT environment.	*Y*	*Implementation*
2.3			Obtain identification, authentication, and access granting procedures for the routers and/or network management software.	*Y*	*Implementation*
2.4			Verify that system administrators gain root access by first logging in to a personal account, then using the substitute user, su command to gain access to the root account. Verify that the system administrator has disabled direct remote root login.	*Y*	*Implementation*
2.5			Verify that users who access root use su for root access and that they belong to the root/wheel/system group.	*Y*	*Implementation*

2.6		and access mechanisms effective (e.g., regular password changes).	View the /etc/passwd file to verify that every account has a password, and that it is not easily guessable. If the password shadow file feature is available, verify that it has been implemented.	*N*	*Implementation*
2.7			Verify that multiple attempts to guess UNIX passwords will lock an account.	*N*	*Implementation*
2.8			Verify that no generic UNIX accounts exist that are not absolute necessary for a commercial product to work, e.g., ensure that no account are named cron, guest, adm, or the name of any department or customer support group.	*N*	*Implementation*
2.9			Verify that the root user is not included in the NIS or NIS+ password file.	*Y*	*Implementation*
2.10			Verify that no users have a .rhosts or .netrc file in their home directory.	*N*	*Implementation*
2.11			Verify that the password file gecos field contains information adequate to identify users.	*N*	*Implementation*
2.12			Verify that users may not unknowingly share their Xwindows display by confirming that the permissions on the xhost command are 700, and that file is owned by root. Also restrict access to Xwindow commands: GrabServer, GrabPointer, GrabKeyboard, ChangeKey	*N*	*Implementation*
2.13			Identify the number of people who know the root password. Verify that their job function requires ongoing unrestricted system access.	*Y*	*Implementation*
2.14			Verify that user account UIDs are assigned excluding key system ranges, preferably over 100. UIDs less than ten (10) are reserved for system accounts and should never be assigned to regular system users.	*Y*	*Implementation*
2.15			Verify that all application users have hard to guess passwords	*Y*	*Implementation*

2.16			Verify that application user passwords expire.	*Y*	*Implementation*
2.17			Verify that dormant application accounts are disabled.	*Y*	*Implementation*
2.18			Verify that multiple attempts to guess application passwords will lock an account.	*Y*	*Implementation*
2.19			Identify NT global groups (other than default groups and system generated groups) and determine the reasons for these groups.	*Y*	*Implementation*
2.20			Ascertain if any changes have been made to the default security privileges of the NT default groups, and the reasons for those changes.	*Y*	*Implementation*
2.21			Examine NT user account details for all users, including administrators' accounts.	*Y*	*Implementation*
2.22			Verify that NT group membership and privileges are appropriate.	*Y*	*Implementation*
2.23			Review the NT user rights that have been allocated to individuals and groups for appropriateness.	*Y*	*Implementation*
2.24			Ascertain if normal production users on the NT network have had their access restricted appropriately through user environment profiles	*N*	*Implementation*
2.25			If logon scripts are used instead of environment profiles to restrict the user's environment within the system determine whether reasons for using scripts are valid.	*N*	*Implementation*
2.26			Check that the NT file security over the user environment profiles and logon scripts prevents unauthorized access or amendment.	*Y*	*Implementation*
2.27			Verify that no users have RAS access.	*Y*	*Implementation*

2.28			Ensure that passwords or stronger authentication mechanisms protect access to the configuration mechanisms of network equipment. Verify that the passwords are shared on a need-to-know basis.	*Y*	*Implementation*
2.29			Test systems within the organization accessible from the wide area network for widespread security vulnerabilities.	*Y*	*Implementation*
2.30			Test selected systems that access the data center through the wide area network for security vulnerabilities. Ensure that they require authentication for network access.	*N*	*Implementation*
2.31			If strategic or confidential data is transferred across the network, verify that logical segmentation is used to maintain minimum access to data required by job function.	*N*	*Implementation*
2.32			Verify that all router ports are secured with passwords.	*Y*	*Implementation*
2.33			Verify that routers do not allow file transfer without identification and authentication.	*Y*	*Implementation*
2.34			Identify default user id and password for platform and application systems and try to gain access.	*Y*	*Implementation*
2.35			Verify that maximum use of network platform and application security features are used to prevent data theft or service disruption due to platform or application corruption.	*Y*	*Implementation*
2.36			Ascertain if any platform has any applications that alter operating system security mechanisms. Assess risks of those applications with respect to operating system security.	*Y*	*Implementation*
2.37			Physically examine all equipment in the scope of the review to verify that there are no dial-up lines and/or modems attached.	*Y*	*Implementation*

APPENDIX A

3.1	Security of Online Access to Data	In an online information technology environment, information services function's management should implement procedures in line with the security policy that provides access security control based on the individual's demonstrated need to view, add, change or delete data.	Determine how user access request is mapped onto system, dial-up, and/or network access. List the individuals responsible for validating access requests for a given sample, dial-ups, or networks, and verify that the access is authorized.	*Y*	*Implementation*
3.2			Determine how user request form is validated before user access request is granted, e.g., if validation is by signature, determine how the signature is validated.	*Y*	*Implementation*
3.3			Ensure that all operating system, database management system, and application security features that limit access to files are configured to ensure that users have the minimum access possible to perform their job functions.	*N*	*Implementation*
4.1	User Account Management	Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included.	Verify that user administration procedures identify specific individuals responsible for validating access requests for each user group, including administrative groups.	*Y*	*Implementation*
4.2			Ensure that authorization procedures rely on first-hand knowledge of individual job responsibility.	*Y*	*Awareness*
4.3			Identify responsibility for user administration. Collect lists of user groups, sample access request forms, process flows for updates to user accounts and process flows for user problem resolution activities.	*Y*	*Implementation*
4.4			For all types of system, network, application, and database accounts, verify that a procedure exists to respond to account-related security incidents.	*N*	*Compliance*
4.5			Verify that user administration procedures to assign individuals to groups ensure consistent configuration. Review automated scripts or configuration parameters.	*Y*	*Implementation*
4.6			Review procedures to immediately deactivate any account found without a password.	*N*	*Compliance*

APPENDIX A

4.7			Review procedures to deactivate any account that is the subject of repeated failed access attempts or was not added by a user administrator.	*N*	*Compliance*
4.8			Review procedures to deactivate any account which has not been used in 90 days.	*N*	*Compliance*
4.9			Review method by which user is given an initial password. Ensure that is it is verbal, with prior authentication of user identity. Ensure that the user is instructed (or forced, system permitting) to change the password once it has been delivered.	*Y*	*Implementation*
4.10			Review method by which user reports a forgotten password, and the method by which it is reset, the user is authenticated, and a new password is delivered. Verify that the process cannot be social-engineered.	*Y*	*Implementation*
4.11			Verify that users cannot defeat password controls.	*Y*	*Implementation*
4.12			Verify that users choose hard passwords, where hard means that passwords are not subject to dictionary attacks.	*Y*	*Implementation*
4.13			Verify that users use numbers and special characters in their passwords where the system allows such usage.	*Y*	*Implementation*
4.14			Verify that users do not change a password to one previously used for the same account.	*Y*	*Implementation*
4.15			Verify that users maintain password lifetime short enough to reduce the risk that passwords will be compromised, and long enough so most users will not need to keep a written record of the password.	*Y*	*Implementation*
4.16			For a sample of users, verify that authorization procedures were followed, that minimum access required for the job function is allowed, that the password has changed since initial configuration, and that the password reflects security awareness.	*N*	*Awareness*

APPENDIX A

4.17			Review employee termination procedures to ensure that they contain procedures for removing computer access and for changing passwords to shared accounts.	*Y*	*Implementation*
5.1	Management Review of User Accounts	Management should have a control process in place to review and confirm access rights periodically.	Identify IT manager responsible for periodically reviewing access rights.	*N*	*Monitoring*
5.2			Review user administration tracking procedures to ensure that they provide a list of users for each system and a list of systems for each user.	*Y*	*Monitoring*
5.3			Verify that periodic audits of system, network, and database passwords are done to ensure that users choose sufficiently hard and unique passwords.	*N*	*Monitoring*
5.4			Verify that there is a one-to-one correspondence between the set of users configured in the system and the list of individuals who have been granted access.	*Y*	*Implementation*
6.1	User Control of User Accounts	Users should systematically control the activity of their proper account(s). Also information mechanisms should be in place to allow them to oversee normal activity as well as to be alerted to unusual activity in a timely manner.	Sample users and determine if awareness activity and documented procedures indefeasibly educates users on risks and responsibilities, including company policies and standards related to system use.	*N*	*Awareness*
6.2			Review user training materials and interview a sample of users.	*N*	*Awareness*
6.3			Verify that users know how to change their own passwords.	*N*	*Awareness*
6.4			Verify that users are given a way to review the last time they accessed a file or logged into a system.	*N*	*Awareness*
6.5			Verify that users know how to report a security incident.	*Y*	*Awareness*
7.1	Security Surveillance	The information services function's security administration should ensure that security activity is logged and any indication of imminent security	Review procedures to identify an account that is the subject of repeated failed access attempts.	*Y*	*Monitoring*
7.2			Verify that automated network monitoring solutions exist where technically feasible.	*Y*	*Monitoring*

7.3		violation is notified immediately to the administrator and is acted upon automatically.	Review user auditing and monitoring procedures to ensure that individual user system and network activity is traceable.	*N*	*Monitoring*
7.4			Ensure that an audit trail is maintained that uniquely identifies administrator access to shared accounts.	*Y*	*Monitoring*
7.5			Verify that all available audit logging features are enabled for key system users and files and audit logs are monitored.	*N*	*Monitoring*
7.6			Review procedures to monitor and respond to users logged on at unexpected times.	*N*	*Compliance*
7.7			Review procedures to monitor and respond to invalid access attempts.	*N*	*Compliance*
7.8			Verify that a procedure exists to identify suspicious files and that duplicate commands are found, investigated, and removed.	*Y*	*Compliance*
7.9			Confirm that the su log file is monitored on a periodic basis.	*Y*	*Monitoring*
7.10			Review procedures to monitor and respond to unexpected file system mounts.	*N*	*Compliance*
7.11			Review procedures to monitor and respond to unexpected network access.	*N*	*Compliance*
7.12			Review procedures to monitor and respond to unsuccessful su attempts to root.	*N*	*Compliance*
7.13			Review procedures to monitor and respond to unexpected system reboots.	*Y*	*Compliance*
7.14			Review procedures to monitor and respond to unexpected changes to system configuration files.	*Y*	*Compliance*
7.15			Review procedures to monitor and respond to unexpected changes to user configuration files.	*N*	*Compliance*

APPENDIX A

7.16			Review the all system security configuration procedures to ensure that system security features are enabled.	*N*	*Implementation*
7.17			Review the auditing that has been established.	*Y*	*Monitoring*
7.18			Identify what audit procedures have been put on files as a default. Determine appropriateness.	*Y*	*Monitoring*
7.19			Verify that invalid attempts to exercise administrative rights are audited.	*N*	*Monitoring*
7.20			Verify that invalid attempts to access domains and shares are audited.	*Y*	*Monitoring*
7.21			Verify that router configuration is monitored frequently enough to detect security incidents.	*Y*	*Monitoring*
7.22			Verify that access to network maintenance activity is logged.	*Y*	*Monitoring*
8.1	Data Classification	Management should implement procedures to ensure that all data are classified in terms of sensitivity by a formal and explicit decision by the data owner according to the data classification scheme. Even data needing "no protection" should require a formal decision to be so designated.	Verify that the information protection policy minimizes risks of liability from managing customer information.	*Y*	*Policy*
8.2			Verify that the information protection policy adequate restricts information on system security access and detection mechanisms.	*Y*	*Policy*
8.3			Review Information Protection Awareness program. Verify that it communicates information protection policy to every member.	*Y*	*Awareness*
8.4			Ensure that there is a comprehensive corporate policy on the protection of information.	*Y*	*Policy*
8.5			Identify person responsible for determining the level of information protection for data available via SoftServe Internet Services.	*Y*	*Strategy*
8.6			Ensure that information protection policy designates roles and responsibilities with respect to levels of information protection.	*Y*	*Policy*

APPENDIX A

8.7			Verify information protection policy compliance of corporate policies and standards with government and regulatory agencies.	*Y*	*Policy*
8.8			Review measures that management takes to enforce information protection policy.	*Y*	*Implementation*
8.9			Determine the level of sensitivity of data stored in data center. Verify that the level set complies with information protection policy.	*Y*	*Implementation*
8.10			Ensure that information protection policy designates information handling (including labeling) procedures for different levels of information protection.	*N*	*Implementation*
8.11			Determine if data center personnel are aware of the sensitivity level of the data stored in the data center, and follows corresponding procedures.	*N*	*Awareness*
9.1	Central Identification and Access Rights Management	Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	Identify organization responsible for centralizing user access right management.	*Y*	*Strategy*
9.2			Sample users and use centralized identification system to determine which systems they should have access. Search for sample users on all systems within scope to verify that centralized record is correct.	*Y*	*Implementation*
9.3			Verify that users are consistently identified on all systems to which they have access.	*N*	*Implementation*
9.4			Verify that users who have access across multiple systems have authorization for the data owner of each system (e.g. no default system access results from centralized management).	*N*	*Implementation*
10.1	Violation and Security Activity	The information services function's security administration should assure that violation and security activity is	Verify that when security incidents occur, the cause is investigated.	*N*	*Compliance*
10.2			If applicable, verify that the user and the user's manager is contacted in the course of the investigation.	*N*	*Compliance*

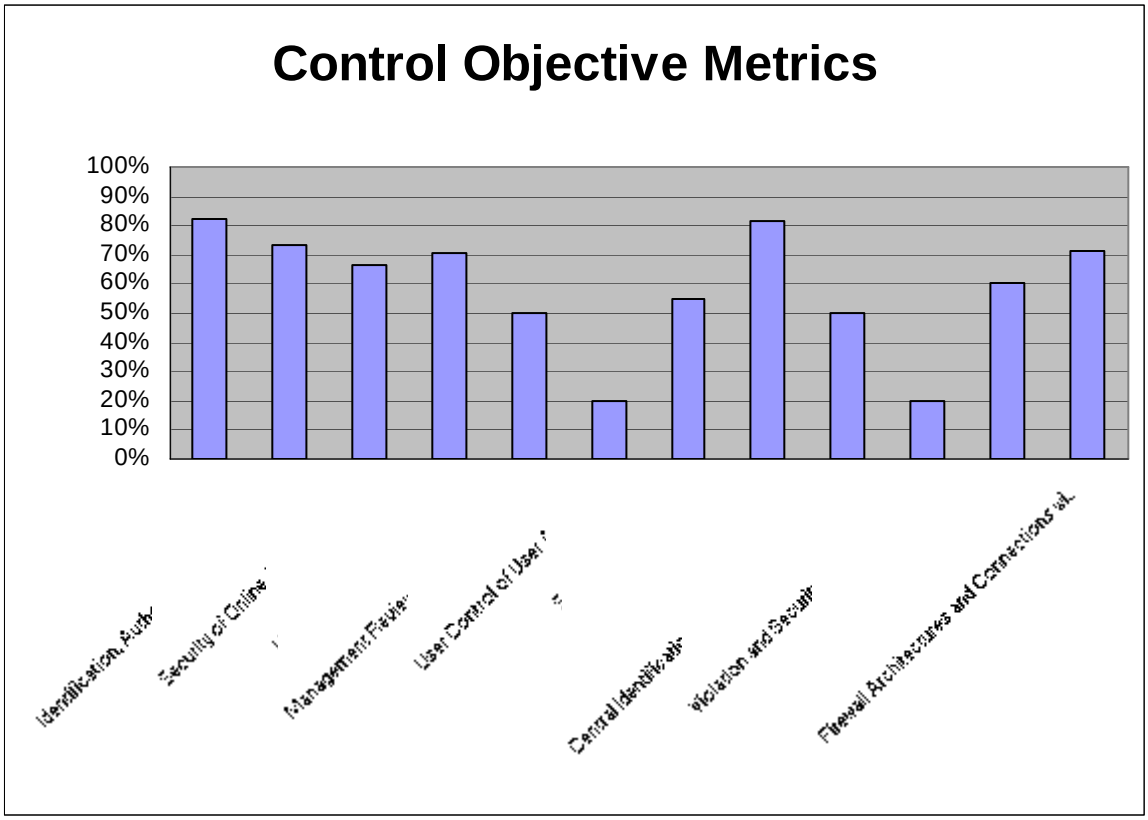
APPENDIX A

10.3	Reports	logged, reported, reviewed and appropriately escalated on a regular basis to identify and resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information should be granted based upon principle of least privilege, or need-to-know.	Observe system security monitoring. Confirm that unexpected user activity is investigated.	*N*	*Compliance*
10.4			Review security logs and alerts to obtain evidence that security incidents are identified.	*Y*	*Monitoring*
10.5			Obtain evidence that security incidents are reported and investigated.	*N*	*Compliance*
11.1	Incident Handling	Management should establish a computer security incident handling capability to address security incidents by providing a centralized platform with sufficient expertise and equipped with rapid and secure communication facilities. Incident management responsibilities and procedures should be established to ensure an appropriate, effective and timely response to security incidents.	Observe system security monitoring. Confirm that unexpected user activity is investigated.	*N*	*Compliance*
11.2			Review the process by which public security alerts are disseminated and require a decision process. Confirm that decisions concerning publicly broadcast security incidents may result in immediate configuration changes.	*N*	*Compliance*
11.3			Ensure that an incident tracking and problem resolution procedure supports the UNIX environment.	*Y*	*Compliance*
11.4			Ensure that an incident tracking and problem resolution procedure supports the NT environment.	*Y*	*Compliance*
11.5			Ensure that an incident tracking and problem resolution procedure supports the telecommunications environment.	*Y*	*Compliance*
12.1	Firewall Architectures and Connections with Public Networks	If connection to the Internet or other public networks exists, adequate firewalls should be operative to protect against denial of services and any unauthorized access to the internal resources; should control any application and infrastructure management flows in both directions; and should protect against denial of	Review network connectivity diagrams that contains detailed components of the network connections of each system under review. Identify all network connections to public, dial-in, or other networks not directly managed by SoftServe, Inc. Determine if traffic routing or filtering is employed to restrict data coming into or out of the Internet Services System environment.	*Y*	*Implementation*
12.2			For each UNIX system under review, use ifconfig -a to determine network connectivity configuration. Verify that it is consistent with network diagrams.	*Y*	*Implementation*

12.3		service attacks.	For each NT system under review, use ipconfig /all to determine network connectivity configuration. Verify that it is consistent with network diagrams.	*Y*	*Implementation*
12.4			Use show ip route to determine network connectivity configuration of each router under review. Verify that it is consistent with network diagrams.	*Y*	*Implementation*
12.5			Verify that the systems under review have no ports accessible from the Internet that are not absolutely necessary for users to run the application.	*Y*	*Implementation*
12.6			Verify that the application does not require any ports open to the Internet that may be exploited for non application system access (e.g.: port 21-ftp, 23-telnet, 22-ssh).	*N*	*Implementation*
12.7			From an Internet connection that is not managed by SoftServe, scan all IP addresses registered to SoftServe. Verify that only expected ports are accessible.	*N*	*Implementation*

APPENDIX B

		#STEPS	Steps where test passed	%PASSED	Steps where test not passed	% NOT PASSED
1	Manage Security Measures	17	14	82%	3	18%
2	Identification, Authentication and Access	37	27	73%	10	27%
3	Security of Online Access to Data	3	2	67%	1	33%
4	User Account Management	17	12	71%	5	29%
5	Management Review of User Accounts	4	2	50%	3	75%
6	User Control of User Accounts	5	1	20%	3	60%
7	Security Surveillance	22	12	55%	10	45%
8	Data Classification	11	9	82%	2	18%
9	Central Identification and Access Rights Management	4	2	50%	2	50%
10	Violation and Security Activity Reports	5	1	20%	4	80%
11	Incident Handling	5	3	60%	2	40%
12	Firewall Architectures and Connections with Public Networks	7	5	71%	2	29%



APPENDIX C

		#STEPS	Steps where test passed	%PASSED	Steps where test not passed	% NOT PASSED
1	Strategy	4	4	100%	0	0%
2	Policy	9	8	89%	1	11%
3	Awareness	11	5	45%	6	55%
4	Implementation	73	55	75%	18	25%
5	Monitoring	18	12	67%	6	33%
6	Compliance	22	6	27%	16	73%