

INFORMATION TECHNOLOGY DEPARTMENT

Bismarck, North Dakota

INFORMATION SYSTEM AUDIT

For the Year ended December 31, 2005

TABLE OF CONTENTS

Executive Summary	2
Independent Auditor’s Report	3
Background Information	5
Objectives, Scope, and Methodology	7
Audit Scope.....	7
Audit Objectives	7
Description of Controls	8
Organizational Controls	8
Planning Controls.....	10
Security Controls.....	11
Human Resource Controls.....	13
Operating Controls.....	14
Incident Management Controls	17
Contingency Planning Controls	17
Information Provided by the State Auditor’s Office	20
Objective – Managing Human Resources	20
Objective – Ensuring Continuous Service	22
Objective – Ensuring Systems Security.....	25
Finding: ITD lacks a formal Security Plan.....	27
Finding: Excessive information is available regarding STAGENet.....	28
Finding: Vulnerability scanning is not being done for all systems	28
Finding: Multiple, sometimes insecure, remote management solutions are in use.....	29
Finding: Lack of a formal incident response program	29
Finding: Firewall configurations out of date	30
Finding: IP and port filtering not used to limit access to critical systems	30
Objective – Managing Facilities	31
Objective – Managing Operations	33
Objective – Ensure Compliance with External Requirements	34
Objective – Managing Performance and Capacity	35
Objective – Assist and Advise Customers	37
Objective – Define Information Architecture	39
Objective – Determine Technological Direction.....	40
Objective – Define IT Organization and Relationships	42
Objective – Manage the IT Investment.....	44
Objective – Communicate Management Aims and Direction	46
Objective – Assess Risks.....	48
Finding: ITD lacks a formal risk assessment framework	48
Objective – Managing Projects	50
Objective – Install and Accredite Systems.....	52
Objective – Manage Changes	53
Objective – Identify and Allocate Costs	54
Objective – Managing Problems and Incidents	55
Objective – Define a Strategic Information Technology Plan	56

June 1, 2006

Honorable John Hoeven, Governor
Members of the Legislative Assembly
Lisa Feldner, Chief Information Officer, Information Technology Department

Transmitted herewith is the general controls audit of the Information Technology Department as of December 31, 2005. The North Dakota Century Code states that the State Auditor “be vested with the duties, powers, and responsibilities involved in performing the post audit of all financial transactions of the state government, detecting and reporting any defaults, and determining that expenditures have been made in accordance with law and appropriation acts.” Audits of the state’s information systems are an important part of these responsibilities.

The audit of the Information Technology Department general controls disclosed eight reportable conditions. Each of these reportable conditions will be explained in detail within this report.

Inquiries or comments relating to this audit may be directed to Donald LaFleur, Information Systems Audit Manager, by calling (701) 328-4744. We wish to express our appreciation to the Information Technology Department for the courtesy, cooperation, and assistance provided to us during this audit.

Sincerely,

Robert R. Peterson
State Auditor

EXECUTIVE SUMMARY

This report is intended to provide interested parties with information sufficient to understand the general controls of the Information Technology Department (ITD) for the period January 1, 2005 to December 31, 2005.

General controls encompass the environment in which all applications are processed. Their purpose is not typically directed to any one application, but to all applications processed at the data center. Effective general controls provide the proper environment for good application controls.

The report is structured according to guidance from the American Institute of Certified Public Accountants' statement of auditing standards number 70 as amended. In accordance with these standards, we obtained a description of controls from ITD and performed testing to ensure the controls were in place and were operating effectively.

Incorporated into this audit was a security study of the state network. Our office contracted with ManTech Security & Mission Assurance, a group of ManTech International Corporation, to conduct this study.

Our audit resulted in the following significant findings:

- ITD lacks a formal Security Plan. (page 27)
- Excessive information is available regarding STAGENet. (page 28)
- Vulnerability scanning is not being done for all systems. (page 28)
- Multiple, sometimes insecure, remote management solutions are in use. (page 29)
- Lack of a formal incident response program. (page 29)
- Firewall configurations are out of date. (page 30)
- IP and port filtering not used to limit access to critical systems. (page 30)
- ITD lacks a formal risk assessment framework. (page 48)

INDEPENDENT AUDITOR'S REPORT

Honorable John Hoeven, Governor
Members of the Legislative Assembly
Lisa Feldner, Chief Information Officer, Information Technology Department

We have examined the accompanying description of controls related to the general controls of the Information Technology Department (ITD). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of ITD's controls that may be relevant to a state agency's internal control as it relates to an audit of financial statements, (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and state agencies applied the controls contemplated in the design of ITD's controls, and (3) such controls had been placed in operation as of December 31, 2005. The control objectives were specified by the management of ITD.

Our examination was performed in accordance with standards for information system audits issued by the Information Systems Audit and Control Foundation, applicable Government Auditing Standards issued by the Comptroller General of the United States, and standards established by the American Institute of Certified Public Accountants. Our examination included those procedures we considered necessary under the circumstances to obtain a reasonable basis for rendering our opinion. We believe that our audit provides a reasonable basis for our opinion

In our opinion, based on our audit, the accompanying description of the aforementioned general controls presents fairly, in all material respects, the relevant aspects of ITD's controls that had been placed in operation as of December 31, 2005. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and state agencies applied the controls contemplated in the design of ITD's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in the Information Provided by the State Auditor's Office, to obtain evidence about their effectiveness in meeting the control objectives described in the Information Provided by the State Auditor's Office during the period from January 1, 2005 to December 31, 2005. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at ITD is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the Governor, Legislative Audit and Fiscal Review Committee, ITD, state agencies, and auditors of the state agencies and is not intended to be and should not be used by anyone other than those specified parties.

Robert R. Peterson
State Auditor

April 4, 2006

BACKGROUND INFORMATION

North Dakota Century Code Section 54-59-02 states “The information technology department is established with the responsibility for all wide area network services planning, selection, and implementation for all state agencies, including institutions under the control of the board of higher education, counties, cities, and school districts in this state. With respect to a county, city, or school district, wide area network services are those services necessary to transmit voice, data, or video outside the county, city, or school district. In exercising its powers and duties, the department is responsible for computer support services, host software development, statewide communications services, standards for providing information to other state agencies and the public through the internet, technology planning, process redesign, and quality assurance.”

North Dakota Century Code Section 54-59-05 states “The department:

1. Shall provide, supervise, and regulate information technology of all executive branch state entities, excluding the institutions under the control of the board of higher education.
2. Shall provide network services in a way that ensures the network requirements of a single entity do not adversely affect the functionality of the whole network, facilitates open communications with the citizens of the state, minimizes the state's investment in human resources, accommodates an ever-increasing amount of traffic, supports rapid detection and resolution of problems, protects the network infrastructure from damage and security breaches, provides for the aggregation of data, voice, video, and multimedia into a statewide transport mechanism or backbone, and provides for the network support for the entity to carry out its mission.
3. May review and approve additional network services that are not provided by the department.
4. May purchase, finance the purchase, or lease equipment or software or replace, including by trade or resale, equipment or software as may be necessary to carry out this chapter. An agreement to finance the purchase of software, equipment, or implementation services may not exceed a period of three years. The department shall submit any intended financing proposal for the purchase of software, equipment, or implementation services under this subsection, which is in excess of one million dollars, to the budget section of the legislative council before executing a financing agreement. If the budget section does not approve the execution of a financing agreement, the department may not proceed with the proposed financing arrangement. The department may finance the purchase of software, equipment, or implementation services only to the extent the purchase amount does not exceed the amount appropriated to the department during that biennium for equipment. Each executive branch agency or institution, except the institutions under the control of the Board of Higher Education, shall submit to the department, in accordance with guidelines established by the department, a written request for the lease, purchase, or other contractual acquisition of information technology. The department shall review requests for conformance with the requesting entity's information technology plan and compliance with statewide policies and standards. If the request is not in conformance or compliance, the department may disapprove the request or require justification for the departure from the plan or statewide policy or standard.
5. Shall provide information technology, including assistance and advisory service, to the executive, legislative, and judicial branches. If the department is unable to fulfill a request for

service from the legislative or judicial branch, the information technology may be procured by the legislative or judicial branch within the limits of legislative appropriations.

6. May request information on or review information technology, applications, system development projects, and application development projects of executive branch agencies.

7. Shall study emerging technology and evaluate its impact on the state's system of information technology.

8. Shall develop guidelines for reports to be provided by each executive branch agency, institution, or department, the institutions under the control of the board of higher education, and agencies of the judicial and legislative branches on information technology in those entities.

9. Shall review the information technology management of executive branch agencies or institutions, including institutions under the control of the board of higher education as provided in section 54-59-13.

10. Shall perform all other duties necessary to carry out this chapter.”

OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Scope

This report is intended to provide interested parties with information sufficient to understand the general controls in place within the Information Technology Department (ITD) during the period from January 1, 2005 to December 31, 2005. This report has been prepared taking into consideration the guidance contained in the AICPA Statement on Auditing Standards No. 70 as amended.

Our audit was conducted in accordance with the *Standards for Information Systems Auditing* issued by the Information Systems Audit and Control Association and *Government Auditing Standards* issued by the Comptroller General of the United States.

Audit Objectives

The objective of this audit was to ensure that controls listed in the Description of Controls were in place and operating effectively.

DESCRIPTION OF CONTROLS

Organizational Controls

ITD is divided into seven divisions (Administrative Services, Software Development, Computer Systems, Telecommunications, Customer Service, IT Planning, Human Resources) to ensure authority and independence from user organizations.

Appropriate roles and responsibilities exist for key processes, including system development life cycle activities, (requirements, design, development, testing), information security, acquisition and capacity planning.

ITD organizational controls ensure appropriate and adequate resources are assigned to implement the organization's policies in a timely manner.

Governance structures are in place to set the direction over the enterprise programs, CJIS, ConnectND, and GIS.

ITD procedures exist to address the need to periodically review and approve key standards, directives, policies and procedures relating to information technology.

ITD's policies and procedures define, document, and maintain a formal philosophy, policies and objectives governing quality of systems and services provided by the organization.

ITD management promotes a positive control environment by example and has accepted full responsibility for formulating, developing, documenting, promulgating, controlling and regularly reviewing policies governing general aims and directives.

ITD establishes the operating budget through the executive planning process (Budget Analysis & Reporting System) and manages budget v. actual expenditures through the centralized PeopleSoft accounting system. The budget is aligned with the enterprise strategic plan. Executive Branch agencies participate in preparing their portions of the IT plan. A goal of the process is to anticipate major infrastructure needs and plan accordingly.

The governor and state legislature set staffing levels biennially in ITD's budget. During the biennial budget process, ITD reviews staffing levels and requests additional FTE as needed.

ITD sets its rates to cover the cost of providing services with a reasonable surplus to finance capital purchases. ITD monitors actual expenditures to billings through the PeopleSoft accounting system cost centers (overhead, systems, programming, telecommunications, IBM central computer, AS/400 computer, micrographic, direct billing, basic phone, in-state long distance, out-of-state long distance, direct billing, and relay service) with the goal of matching billings to expenditures within each cost center.

ITD rate setting process and annual report include comparisons to similar rates charged by other states and private sector providers to ensure that the rates are competitive with similar services offered by other states and the private sector.

ITD manages its legal and contractual responsibilities and liabilities through ongoing internal monitoring of legislation, contracts, and regulatory changes.

ITD performs an annual physical inventory of fixed assets within the department.

ITD obtains independent assurance of compliance with laws, regulatory requirements and contractual obligations through audit functions conducted by the Office of the State Auditor. The State Auditor performs routine examinations of ITD's financial, performance, and IT controls.

ITD's Procurement Officer reviews RFP's and contracts for compliance with policies and procedures over hardware and software acquisition, implementation, and maintenance. State procurement rules govern the acquisition process - acquisitions must comply with state standards unless an exception is granted.

ITD utilizes the Attorney General standard contracts where possible, and has established service level agreements with key providers that provide contracted services to ITD. ITD's large-dollar contracts are reviewed and approved by the Attorney General. In addition, ITD follows the RFP and state procurement process.

ITD evaluates the internal control processes within the department on an ongoing basis, through management meetings, budgetary review, external audits - including SAS70 reviews, internal security assessment, and through internal assessment of policies and procedures.

ITD management and staff meet on a scheduled basis to discuss internal operations and direction. Management and supervisors meet weekly, and all ITD staff meet twice per year.

ITD publishes an annual report which includes: benefits realized from investment in technology; a status report on large and small projects; ITD's performance against goals: ITD's service rates (20 rates that generate 90% of ITD revenue) which are compared with costs charged by similar organizations; the strategic planning process; an update on internal performance measures, and future IT initiatives. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee. The report is also available at ITD's website under "Publications".

ITD publishes a quarterly agency newsletter titled "Information Link." ITD also coordinates the "IT Directional Meeting" for executive branch agency representatives to inform them on current initiatives and issues.

ITD conducts an annual customer survey to ensure the department is meeting customers' expectations. The survey allows customers to rate their satisfaction with the services provided by ITD and to suggest improvements. Survey areas are software development, computer services, E-mail services, support, telephone services, network service, records management, IT planning services, and an overall ITD survey. Results are published in ITD's strategic plan.

ITD meets with key customers on a monthly or quarterly basis to gather information about future plans and needs.

Planning Controls

Per NDCC 54-59-07, the Statewide Information Technology Advisory Committee (SITAC) advises ITD regarding statewide IT planning, including providing e-government services for citizens and businesses, developing technology infrastructure to support economic development and workforce training, and developing other statewide IT initiatives and policy.

ITD has established an Enterprise Architecture process. This process relies on participation of agency representatives. Each agency that is interested is invited to participate in various domain teams that study specific technology domains and provide proposals to the Architecture Review Board (ARB) and State Information Technology Advisory Committee (SITAC). This process addresses enterprise technology issues and results in state standards, policies and guidelines.

ITD is legislatively mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. The Enterprise Architecture (EA) process promotes state agency participation with ITD in setting future direction of information technology in the state of North Dakota.

A Compliance with Standards section is included in agency IT plans. Agencies indicate the status of their compliance with standards and policies and if not in compliance, provide an approved waiver request and provide plans to bring the agency into compliance.

ITD maintains a biennial Strategic Business Plan, outlining goals and objectives for each division, and follows a methodology for measuring progress toward the goals outlined in the business plan, per NDCC 54-59-06.

ITD's Strategic Business Plan outlines goals and tactics for each division. Progress towards these goals and tactics is monitored on a quarterly basis by the Chief Information Officer and reported to the Legislative Information Technology Committee.

ITD evaluates progress toward the goals outlined in the strategic plan, and publishes the results in the annual report (balanced scorecard). ITD also tracks performance metrics internally, both at the department and division levels.

ITD's strategic planning process outlines the rates and funding mechanisms necessary to finance the proposed activities of the department, in accordance with NDCC 54-59-06.

ITD's strategic planning process takes into account organizational changes, technology evolution, regulatory requirements, business process reengineering efforts and staffing requirements.

ITD's technological infrastructure is maintained on an ongoing basis, takes into account current and future technology trends and regulatory conditions, and is compared with the IT long and short range plans.

ITD manages risks associated with individual procurement contracts based on the dollar value and by requiring agencies to provide documented requests for information technology.

ITD provides guidelines for agencies to follow in preparing their technology plan, reviewing the plans for compliance with statewide policies or standards, resolving conflicting directions among plans, and assembling the agency plans into a statewide plan to be submitted to the members of the Legislative Assembly. ITD also reviews and approves technology acquisitions for conformance with the agency's IT plan and compliance with statewide policies and standards.

Each state entity is responsible for preparing its budget request based on its IT plan and must describe in detail how the IT plan relates to the budget request. Similarly, the executive budget recommendation must include detailed information about the relationship to the agency's IT plan.

State agency IT Plan updates are to be done as needed to communicate the IT direction and resource needs of the agency. The IT plan must be updated if the goals and objectives change, if a major project is added or deleted, or at the request of ITD.

ITD's annual customer survey includes a section on information technology planning. ITD's Information Technology Planning Analyst reviews the surveys and meets with agencies to assess the IT planning process.

North Dakota Century Code Section 54-35-15.2 provides that the Legislative Information Technology Committee shall "review the cost-benefit analysis of any major information technology project (=> 250K per biennium or => \$500K in total) of an executive or judicial branch agency" and "perform periodic reviews to ensure that a major information technology project is on its projected schedule and within its cost projections."

ITD's large project reporting has five phases: business case, project plan, quarterly status reports, summary status report, and post-project analysis. In the business case phase the agency defines the business requirements, does a cost/benefit and risk analysis, establishes a project manager and executive steering team, and presents this to the Legislative Information Technology Committee. ITD has established guidelines for making the business case. The project plan is to be prepared based on industry "best practices." ITD encourages the use of the Project Management Institute (PMI) format. Quarterly reports define the scope of the project and state the project schedule. The report compares budgeted to actual costs and outlines current progress and issues. ITD's planning analysts review the report and present summary status reports to the Legislative Information Technology Committee each quarter. The post-project analysis assesses whether the project accomplished its business objectives.

ITD's large project oversight process ensures the project plan includes a formal system development life cycle for system development and installation, including requirements definition, coding, testing, conversion, training, and documentation.

ITD's large project oversight process incorporates quality management processes within the project plan.

Security Controls

ITD's Administrative Services Division has formally assigned to a security officer organization wide responsibility for formulation of internal control and security (logical and physical) policies and procedures.

ITD's security and internal control framework specifies the internal control policy, purpose and objectives, management structure, scope within the organization, assignment of responsibilities, and definition of penalties and disciplinary actions associated with noncompliance.

All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business results or the business use of the object. There is one and only one owner for each object - the owning agency appoints an agency security officer who is responsible for controlling access rights.

ITD's policies and procedures address the classification of data, including security categories and data ownership, and access rules for the classes of data are clearly defined.

ITD maintains logical security access controls at the mainframe and mid-tier platform levels and maintains a history of user id operating system level access. Controls include:

- Invalid sign on attempt lockout
- Unauthorized attempts to access system resources
- Resource access privileges by user id (mainframe)
- Authorized security definitions and rule changes
- History of up to 5 passwords and limits on password reuse.
- Password standards, as defined by the Enterprise Architecture Security Domain Team, are implemented at the mainframe and mid-tier operating system

ITD, through the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address:

- Prevention and detection of computer viruses, and installation of virus prevention software and critical updates.
- Firewall intrusion prevention and detection mechanisms over the state network environment, including proactive intrusion detection and passive review of intrusion attempts
- Business-only use of computer resources, including fax and voice mail
- Remote access

ITD enforces Windows Active Directory standards internally, over user authentication within their internal Windows and web-based applications. Agency security personnel are responsible for establishing and monitoring active directory parameters, in accordance with EA Security Domain Team recommendations, for user authentication and data access privileges within their own directories of the state network.

ITD has implemented information authentication and integrity standards over networked resources through Active Directory, thereby providing a single network sign-on within a single network domain. ITD provides the Domain controllers and Global Catalog servers for authentication services.

ITD's Network Firewall Group supports maintenance of firewalls based upon authorized service requests passed through the Work Management System after review by the ITD Security division. ITD's policy rules over firewall control is "lock down all, and open up to only authorized hosts that require access" rather than "allow all, except for.....".

ITD's Security team reviews firewall activity logs each following business day for reported "failed connection" attempts. The review looks for repeated attempts to break one or multiple firewalls within the network - if found, the Security Officer reports the incident(s) to the Network Firewall Group to lock the offender from accessing the outermost state network firewall.

Active Directory login credentials are encrypted during transmission.

ITD deploys SSL encryption where appropriate.

ITD has implemented Intrusion Detection Systems and performs regular vulnerability assessments on its computing and network infrastructure

ITD utilizes an on-line Work Management System where authorized users can request adds, changes or deletes to access rights for systems maintained by ITD.

On an annual basis, ITD contacts the Security Officers at each agency to review the access rights granted to each agency. This is an addition to the daily and monthly access reports sent to each agency.

ITD's Computer Operations Team maintains the RACF and SMF central database security software that controls access to agency-owned datasets, library files, source code, etc. ITD Computer Operations Team also administers the Work Management System (WMS) via DBA's, as well as the internal security tools for general level access auditing within SQL-server and Oracle databases. Note: Agencies are responsible for establishing the internal controls and business process over data input, processing, and output for transaction activity conducted at the agency site.

The Highway Patrol provides maintenance and security of the capitol complex, including the offices and facilities of ITD.

ITD's Security Officer supports the Highway Patrol administration procedures as specific to ITD.

Human Resource Controls

ITD uses the ND Human Resource Management Services division job classifications for all positions, which detail the minimum qualifications necessary for each position. A position information questionnaire (PIQ) is used to further define the position qualifications and personnel selection criteria.

ITD recruitment practices include participating at technical expos and college job fairs, advertising available positions on the ITD and Central Personnel web-sites, as well as in the print media and with Job Service of North Dakota.

ITD performed criminal background checks on all employees and recorded fingerprints in June 2003. ITD performs an annual update of the employee information and has defined procedures to perform follow-up background checks on the employees every five years. The Bureau of Criminal Investigations is contracted to perform this service for ITD.

On an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the confidentiality requirements of the data they handle. In addition there is an annual acknowledgement of seven other policies relevant to the department.

ITD management is committed to personnel training and career development. Employee training is the responsibility of the employee and their manager. ITD division managers may specify training needs in an employee's annual evaluation or approve requests for training submitted by the employee. Training requests, status, and costs are tracked internally. Training costs are tracked by section, and averaged by FTE for budget tracking/estimating purposes.

ITD surveys internal employees to identify and assess any performance issues and establish internal goals / objectives.

ITD will pay for the testing required for professional certifications and upon completion will provide a one-time bonus to the employee.

ITD employee resignation procedures follow a documented exit process to return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation.

ITD issues a pre-action notice to employees subject to termination, and places the employee on administrative leave. The employee must return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation or termination notice.

ITD policies and procedures are published and made available to ITD employees on the intranet.

ITD follows the NDCC and policies developed by OMB regarding annual leave accrual and cut-off dates for leave balances above 240 hours.

ITD's Human Resources Division has established policies and procedures for the evaluation and re-evaluation of IT position descriptions.

ITD's Human Resources Division maintains policies and procedures in accordance with applicable laws and regulations.

ITD procedures ensure that ongoing cross-training and backup of staff for critical job functions occurs.

Operating Controls

ITD's Computer Facility environmental controls include fire suppression, raised floors, water detectors, smoke alarms and air conditioning units. Semi-annual tests are done to verify correct alarm operation. Facility Management Division provides a UPS for back-up power and power regulation, and a generator for extended power loss. The UPS is tested semi-annually and the generator is tested weekly.

ITD's Computer Facility includes a separate agency server room where agencies can store their network / application servers. The servers are backed up and ITD assumes maintenance of the server operating system. Agency personnel may obtain limited access to the agency server room from ITD security personnel.

ITD's Computer Facility agency server room has a raised floor, smoke detectors, air conditioning, and security camera. Agency personnel are allowed access to the room through their key cards.

ITD schedules mainframe / mid-tier operating system down-time with agency IT coordinators, posts the outage schedule on the website, and provides web-based subscription service for automated email notifications of future scheduled maintenance activities.

ITD monitors computer and network operations performance based on assessments of individual systems and the knowledge of support and project teams, tools such as graphs, operators' knowledge, and available performance capacity system software. Performance management reports include e-mail messages by platform for e-mail servers, CPU utilization, DASD I/O per second, memory pages per second, and disk capacity for the mainframe.

ITD's mainframe and AS/400 platforms include redundant hardware controls to ensure continued operations in event of a part failure, and the mainframe O/S software will contact IBM technical service support as necessary.

ITD critical servers have redundant power supplies and all disk systems utilize RAID to ensure no data loss due to hard drive failures.

ITD's computer operations include instructions for operators such as checklists, IPL instructions, shut down procedures, restart procedures, on-call lists, console commands, and other miscellaneous memos.

ITD uses Operations Planning and Control Scheduler (OPC) to schedule nightly jobs on the mainframe. Production control employees or agency personnel can schedule jobs in OPC. Production control specialists review the nightly job schedules. Jobs that abend (abnormally end) will send a message to the mainframe master console. Operators will then contact on call programmers and responsible agency personnel to fix the job.

ITD computer operations utilizes IBM's Syslog (System Log) to log activity on the mainframe.

ITD completed deployment of the Work Management System (WMS) to state agency users in November 2004. ITD developed this web-based system internally to provide a "one-stop center" for customers to request ITD software development services, and enhance ITD's project management, time recording, and billing services.

ITD has implemented Mercury SiteScope infrastructure monitoring software over the state network platform to monitor performance characteristics (utilization, response time, usage and resource availability). ITD has configured SiteScope to automatically detect and report/record incidents over network resources.

ITD's Computer Systems Division has implemented ongoing procedures to monitor performance and capacity of the mainframe and mid-tier operating systems within the computer facility, and maintains historical statistics for future capacity planning and budgetary planning purposes.

ITD's Computer Systems Division maintains the configuration inventory (hardware, O/S software, applications software, facilities and data files) through HP's Systems Insight Manager software configuration tools, Altiris and the CIS Database (ITD application for hardware).

ITD's Computer Systems Division utilizes Quest Stat Application Change Management (ACM) for PeopleSoft tools for patch management, versioning capabilities, process management and change request tracking over the ConnectND application. Other QA/change control/developer tools include IBM's Rational ClearCase and Cool:Gen

ITD's Computer Systems Division database administrators use the Work Management System to track customer change requests and document software changes over Websphere, .NET, and agency database applications maintained by ITD.

ITD's Computer Systems Division manages desktop computer configurations using Altiris Client Management Suite tools for desktop and notebook computers. In accordance with ITD Policy DT002-04.1, the Altiris Client Management Suite provides the ability to connect, load software, load patches, do troubleshooting, and get asset information from a remote site. Records of installed software may be obtained through Altiris. ITD's "acceptable use policy" addresses unauthorized software installations on state-owned computers by employees.

ITD validates the software installed on mainframe / midtier / desktop platforms agrees to the licensed inventory when renewing annual maintenance agreements with the vendor.

ITD provides physical security, backup/recovery, O/S maintenance services, and production processing services for agency applications that reside in the Computer Operations Facility. Agencies are responsible for managing their data processed through the applications. ITD provides the scheduling software agencies may use to schedule regular job runs. System output printed at ITD's computer facility is secured from unauthorized access.

ITD's Production Control team provides production processing services for agency applications residing in the computer facility. These include: production control reports through CA:Librarian, central print and storage of system output until picked up by authorized agency personnel, maintenance of IBM's Syslog for 6 months, transfer and handling of agency inventory media, "zero-ing" of all hard drives for all desktops and other internal drives.

ITD's Magstar - Librarian and LTO 3 Library tape backup systems include automated cleaning and write verification processes.

ITD's Computer Operations and Production Control teams ensure operations are adequately managed by maintaining and/or following documented operational instructions, managing and evaluating performance statistics over hardware and peripheral capacity utilization and performance, ensuring equipment is maintained on schedule, and ensuring a physical and logical segregation of source and object, test / development / production libraries.

ITD manages changes to application software by documenting, prioritizing, and tracking system changes requests from users. The change process is monitored by ITD for improvements in acknowledgment, response time, response effectiveness and user satisfaction with the process.

ITD Distributed Systems utilizes a web-based change management system to log changes. Changes are logged in the system and approved by the Computer Systems Manager or the System Architect.

ITD utilizes separate test and production environments critical systems. Some systems have separate development environments as well. New applications or application changes are

tested by users in the separate test platform or region. After acceptance ITD system administrators and or DBA's migrate the changes to production.

Incident Management Controls

ITD's Customer Service Division Support Center operates a help desk and provides a full-service central repository for customers to report problems, ask questions, request information, and receive back resolutions and answers in an organized and expedient manner.

ITD's Customer Service Division staff include the Customer Service Director, Service Center Manager, one full-time Service Management Software Analyst and five full-time Service Desk Analysts. Service Desk Analysts cover 7am - 5pm M-F and rotate on-call Saturday morning through Monday 7am. Computer Operations staff cover calls 5pm - 7am M-F.

ITD's Support Center receives requests via telephone and email, and logs / tracks the requests through HEAT from FrontRange Solutions - Incident Management System. ITD has implemented HEAT with the following control parameters:

- Defined assignment groups, supervisors, and role-specific security
- Defined incident categories, call-types, sub-call-types, and incident priority matrix
- Defined detail screens to gather call-type specific information, and customer-specific details
- Acknowledgement, escalation, and communication procedures
- Monthly reporting & analysis, incident records archived 3 years

ITD's Customer Service Division performs monthly reporting and analysis of incident records (HEAT) and Automatic Call Distribution (ACD) telephone system records, and tracks performance measures based upon key indicators.

ITD's Customer Service Division has implemented the Continuous Improvement Cycle based upon IT Infrastructure Library (ITIL) best practices for Service Desks, Incident Management, and Change Management.

ITD's Computer Systems Division utilizes HEAT incident tracking system to address issues - escalation procedures are being followed and appropriate in resolving problems.

Contingency Planning Controls

(Process implemented after audit reporting period) - ITD maintains a disaster recovery hotsite in Mandan, ND to replace the existing recovery hotsite in Boulder, Colorado, by the end of calendar year 2005. The hotsite facility will provide true replication of critical application servers and houses full daily backup tapes for file recovery or complete system restore, if needed.

ITD performs a yearly test of the Disaster Recovery Plan at the hotsite facility. Tests include restoring the IBM S/390 mainframe, AS/400, and UNIX system platforms, and establishing the network / communications with the disaster recovery site. Test procedures and results are documented and reviewed by ITD's Contingency Planning Specialist, who coordinates any necessary changes to the Disaster Recovery Plan.

ITD's disaster recovery tests provide for a mix of experienced and non-experienced personnel involvement on each recovery test. External agency personnel also participate in the testing process to validate recovery of their applications.

ITD's off-site storage facility includes a back-up of the current operating system, system/390 (mainframe) start-up instructions, one copy of the disaster recovery plan, and a recovery priority list of mainframe and mid-tier applications. A copy of the back-up tapes is kept at the off-site storage facility.

ITD's off-site storage facility is physically secured through a combination vault door and cement walls and ceiling. There are no windows and only a small vent for air conditioning. There is a fire extinguisher located inside the off-site vault. There are no formal annual inspections; however, ITD personnel use the vault daily. ITD updates the vault combination upon every employee turnover, or annually at a minimum.

ITD contracts with IBM BRCS for hot-site recovery services in Boulder, CO, over mainframe, mid-tier, telecom, and network operations. This contract expires in spring 2006 and will be replaced by a self-controlled second site in the Bismarck area.

ITD's Contingency Planning Specialist is responsible for establishing and maintaining ITD's disaster recovery plan through participation in the Continuum of Government Team, formed in June 2002, headed by the Office of Management and Budget - Risk Management Division. This team is tasked with establishing a uniform web-enabled relational database software application from Strohl Systems Group, Inc. - Living Disaster Recovery Planning System (LDRPS).

ITD maintains a consistent philosophy and framework over business contingency plan development and prioritizes internal and statewide applications with respect to criticality and timeliness of recovery, as mandated by the Continuum of Government Team, through criteria listed in the LDRPS system.

ITD defines specific roles and responsibilities over continuity planning within the LDRPS and determines the specific test, maintenance and update requirements for the contingency plan.

ITD's disaster recovery plan maintained in LDRPS includes the following:

- Emergency procedures to ensure the safety of staff members, as required by the COG Team.
- Roles & Responsibilities including team members and leaders, task assignments, vendor and customer contact information, administrative support personnel, and site-specific personnel.
- Identification of all software applications required to restore a business function and the recovery time objective (RTO) for each application.
- Administrative functions for communicating and providing support services such as benefits, payroll, and external communications.
- Specific equipment and supply needs.
- Training / awareness of individual and group roles.
- Itemization of contract service providers, services, and response expectations.
- Logistical information on location of key resources such as O/S, applications, data files, operating manuals, etc.
- Current contact information of key personnel.
- Business resumption alternate work locations for all users once IT resources are available.

ITD ensures agency requirements over continuity planning are met and coordinates with four primary agencies (Bank of North Dakota, Department of Transportation, Department of Human Services and Tax Department) to identify specific federal regulatory requirements. ITD works with those agencies to meet the requirements.

ITD's contingency plan, outlined in LDRPS, includes the identification of resources needed to recovery a business function. ITD cross trains employees to perform various disaster recovery tasks.

ITD's data center, network operations center, and second data center run off of UPS and have back up power generators

INFORMATION PROVIDED BY THE STATE AUDITOR'S OFFICE

Objective – Managing Human Resources

To acquire and maintain a motivated and competent workforce and maximize personnel contributions to the IT processes.

Controls

ITD uses the ND Human Resource Management Services division job classifications for all positions, which detail the minimum qualifications necessary for each position. A position information questionnaire (PIQ) is used to further define the position qualifications and personnel selection criteria.

ITD's Human Resources Division maintains policies and procedures in accordance with applicable laws and regulations.

ITD recruitment practices include participating at technical expos and college job fairs, advertising available positions on the ITD and Central Personnel web-sites, as well as in the print media and with Job Service of North Dakota.

ITD performed criminal background checks on all employees and recorded fingerprints in June 2003. ITD performs an annual update of the employee information and has defined procedures to perform follow-up background checks on the employees every five years. The Bureau of Criminal Investigations is contracted to perform this service for ITD.

ITD surveys internal employees to identify and assess any performance issues and establish internal goals / objectives.

ITD will pay for the testing required for professional certifications and upon completion will provide a one-time bonus to the employee.

ITD procedures ensure that ongoing cross-training and backup of staff for critical job functions occurs.

ITD employee resignation procedures follow a documented exit process to return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation.

ITD issues a pre-action notice to employees subject to termination, and places the employee on administrative leave. The employee must return keys, door access cards, and all ITD equipment. Account privileges, email and voicemail services are disabled upon resignation or termination notice.

On an annual basis, ITD employees are required to sign an Acknowledgment of Secrecy Provision to ensure they are aware of the confidentiality requirements of the data they handle. In addition there is an annual acknowledgement of seven other policies relevant to the department.

ITD follows the NDCC and policies developed by OMB regarding annual leave accrual and cut-off dates for leave balances above 240 hours.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding hiring, training, and termination procedures.

We selected a sample of ten current employees to check that they had criminal background checks, had signed the yearly acknowledgement of understanding of ITD's policies and security responsibilities, had professional certifications appropriate for their position, and had received adequate training for their position.

We performed an analytical review of ITD leave balances to ensure they appeared adequate and in-line with policies.

ITD has a defined recruitment and hiring process. ITD's recruiting efforts include posting job announcements on America's Job Bank and in North Dakota newspapers. For some positions ITD advertises in larger cities in nearby states. ITD rates applicants according to a rating system that can be different for each position. ITD selects top candidates for interview. The interview team consists of a Human Resources person, the division director, and the supervisor of the position. After interviews the team ranks candidates and Human Resources contacts references for the top candidate. Following the reference check, ITD contacts the Attorney General's Office to obtain a background check.

ITD has two approaches to training. First, they prepare an educational plan for every employee. The employee and their supervisor update the plan during the employee's annual performance appraisal. Second, if they identify deficiencies, they create a performance improvement plan that clearly lays out management's expectations for the employee.

ITD developed a termination checklist that identifies who is responsible for each step. Each step is checked off and initialed when completed. For involuntary terminations, ITD increases their security level by locking all doors and requiring valid key cards to access them.

Our test of ten employees showed that all had criminal background checks, signed yearly acknowledgement of reading and understanding ITD policies and security responsibilities, had appropriate certifications for their position, and received appropriate training for their position during the audit period.

Our test of leave balances showed ITD follows OMB policy regarding annual leave balances.

Conclusion

We conclude that ITD has met the objective of managing human resources.

Objective – Ensuring Continuous Service

To make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption.

Controls

ITD performs a yearly test of the Disaster Recovery Plan at the hot site facility. Tests include restoring the IBM S/390 mainframe, AS/400, and UNIX system platforms, and establishing the network / communications with the disaster recovery site. Test procedures and results are documented and reviewed by ITD's Contingency Planning Specialist, who coordinates any necessary changes to the Disaster Recovery Plan.

ITD's disaster recovery tests provide for a mix of experienced and non-experienced personnel involvement on each recovery test. External agency personnel also participate in the testing process to validate recovery of their applications.

ITD's off-site storage facility includes a back-up of the current operating system, system/390 (mainframe) start-up instructions, one copy of the disaster recovery plan, and a recovery priority list of mainframe and mid-tier applications. A copy of the back-up tapes is kept at the off-site storage facility.

ITD contracts with IBM BRCS for hot site recovery services in Boulder, CO, over mainframe, mid-tier, telecom, and network operations. This contract expires in spring 2006 and will be replaced by a self-controlled second site in the Bismarck area.

ITD's Contingency Planning Specialist is responsible for establishing and maintaining ITD's disaster recovery plan through participation in the Continuum of Government Team, formed in June 2002, headed by the Office of Management and Budget - Risk Management Division. This team is tasked with establishing a uniform web-enabled relational database software application from Strohl Systems Group, Inc. - Living Disaster Recovery Planning System (LDRPS).

ITD maintains a consistent philosophy and framework over business contingency plan development and prioritizes internal and statewide applications with respect to criticality and timeliness of recovery, as mandated by the Continuum of Government Team, through criteria listed in the LDRPS system.

ITD defines specific roles and responsibilities over continuity planning within the LDRPS and determines the specific test, maintenance and update requirements for the contingency plan.

"ITD's disaster recovery plan maintained in LDRPS includes the following:

- Emergency procedures to ensure the safety of staff members, as required by the COG Team.
- Roles & Responsibilities including team members and leaders, task assignments, vendor and customer contact information, administrative support personnel, and site-specific personnel.
- Identification of all software applications required to restore a business function and the recovery time objective (RTO) for each application.
- Administrative functions for communicating and providing support services such as benefits, payroll, and external communications.
- Specific equipment and supply needs.
- Training / awareness of individual and group roles.
- Itemization of contract service providers, services, and response expectations.

- Logistical information on location of key resources such as O/S, applications, data files, operating manuals, etc.
- Current contact information of key personnel.
- Business resumption alternate work locations for all users once IT resources are available."

ITD ensures agency requirements over continuity planning are met and coordinates with four primary agencies (Bank of North Dakota, Department of Transportation, Department of Human Services and Tax Department) to identify specific federal regulatory requirements. ITD works with those agencies to meet the requirements.

ITD's contingency plan, outlined in LDRPS, includes the identification of resources needed to recovery a business function. ITD cross trains employees to perform various disaster recovery tasks.

Future Process - ITD maintains a disaster recovery hot site in Mandan, ND to replace the existing recovery hot site in Boulder, Colorado, by the end of calendar year 2005. The hot site facility will provide true replication of critical application servers and houses full daily backup tapes for file recovery or complete system restore, if needed.

Tests of Operating Effectiveness and the Results of Those Tests

We examined ITD's disaster recovery plan.

We reviewed the results of the latest test of the disaster recovery plan.

We tested personnel assignments for the last five tests to ensure staff was being rotated.

We inspected the backup site to ensure it contained the necessary information.

We interviewed ITD personnel regarding meetings with the four primary agencies.

We interviewed key personnel from the disaster recovery plan to ensure they were aware of the plan, understood their role, and had participated in training or testing of the plan.

ITD's disaster recovery plan contains the necessary information for proper recovery. ITD based their current disaster recovery plan on having the hot site in Boulder, Colorado. ITD discontinued their contract for the Boulder, Colorado hot site December 31, 2005 and is transitioning to a backup site in Mandan.

ITD conducted the last disaster recovery plan test in 2004. ITD did not test during 2005 since they discontinued the contract for the Boulder, Colorado hot site.

The review of personnel assignments for the last five tests showed that ITD is rotating personnel involved in the test to ensure several employees have experience. Our test also showed that personnel from user agencies are participating in the tests.

We verified that there was a copy of the disaster recovery plan in the backup site. The contingency planner stated that they keep a back-up of the current operating system, which is a snapshot of the mainframe. He stated that this is kept on tapes that are brought over to the backup site every Monday.

Minutes are not taken for the meetings with the four primary agencies. Discussions with ITD indicate that the meetings are not formal and are held only as needed.

Our interviews of key personnel indicated that the employees were aware of the disaster recovery plan, understood their roles, and the employees received training or participated in tests. One employee indicated that he was not sure how the plan defined his role. Since that employee participated in the 2004 test of the plan we did not consider this an error because he performed the role during the test and was just unaware of the exact language in the plan.

Conclusion

We conclude that ITD has met the objective of ensuring continuous service.

Objective – Ensuring Systems Security

To safeguard information against unauthorized use, disclosure, modification, damage, or loss.

Controls

ITD has established an Enterprise Architecture process. This process relies on participation of agency representatives. Each agency that is interested is invited to participate in various domain teams that study specific technology domains and provide proposals to the Architecture Review Board (ARB) and State Information Technology Advisory Committee (SITAC). This process addresses enterprise technology issues and results in state standards, policies and guidelines.

A Compliance with Standards section is included in agency IT plans. Agencies indicate the status of their compliance with standards and policies and if not in compliance, provide an approved waiver request and provide plans to bring the agency into compliance.

ITD is legislatively mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. The Enterprise Architecture (EA) process promotes state agency participation with ITD in setting future direction of information technology in the state of North Dakota.

ITD's security and internal control framework specifies the internal control policy, purpose and objectives, management structure, scope within the organization, assignment of responsibilities, and definition of penalties and disciplinary actions associated with noncompliance.

"ITD maintains logical security access controls at the mainframe and mid-tier platform levels and maintains a history of user id operating system level access. Controls include:

- Invalid sign on attempt lockout
- Unauthorized attempts to access system resources
- Resource access privileges by user id (mainframe)
- Authorized security definitions and rule changes
- History of up to 5 passwords and limits on password reuse.
- Password standards, as defined by the Enterprise Architecture Security Domain Team, are implemented at the mainframe and mid-tier operating system"

"ITD, through the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address:

- Prevention and detection of computer viruses, and installation of virus prevention software and critical updates.
- Firewall intrusion prevention and detection mechanisms over the state network environment, including proactive intrusion detection and passive review of intrusion attempts
- Business-only use of computer resources, including fax and voice mail
- Remote access"

ITD enforces Windows Active Directory standards internally, over user authentication within their internal Windows and web-based applications. Agency security personnel are responsible for establishing and monitoring active directory parameters, in accordance with EA Security Domain Team recommendations, for user authentication and data access privileges within their own directories of the state network.

ITD completed deployment of the Work Management System (WMS) to state agency users in November 2004. ITD developed this web-based system internally to provide a "one-stop center" for customers to request ITD software development services, and enhance ITD's project management, time recording, and billing services.

ITD has implemented information authentication and integrity standards over networked resources through Active Directory, thereby providing a single network sign-on within a single network domain. ITD provides the Domain controllers and Global Catalog servers for authentication services.

ITD provides physical security, backup/recovery, O/S maintenance services, and production processing services for agency applications that reside in the Computer Operations Facility. Agencies are responsible for managing their data processed through the applications. ITD provides the scheduling software agencies may use to schedule regular job runs. System output printed at ITD's computer facility is secured from unauthorized access.

ITD's Computer Operations Team maintains the RACF and SMF central database security software that controls access to agency-owned datasets, library files, source code, etc. ITD Computer Operations Team also administers the Work Management System (WMS) via DBA's, as well as the internal security tools for general level access auditing within SQL-server and Oracle databases. Note: Agencies are responsible for establishing the internal controls and business process over data input, processing, and output for transaction activity conducted at the agency site.

Active Directory login credentials are encrypted during transmission.

ITD deploys SSL encryption where appropriate.

ITD has implemented Intrusion Detection Systems and performs regular vulnerability assessments on its computing and network infrastructure

ITD utilizes an on-line Work Management System where authorized users can request adds, changes or deletes to access rights for systems maintained by ITD.

On an annual basis, ITD contacts the Security Officers at each agency to review the access rights granted to each agency. This is an addition to the daily and monthly access reports sent to each agency.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's Security and Internal Control Framework

We reviewed IT standards related to security.

We interviewed ITD personnel regarding the submitting and handling of agency security requests.

We interviewed ITD personnel regarding the review and retention of security logs.

ITD's Security and Internal Control Framework was a set of standards and procedures that ITD developed prior to the Enterprise Architecture process being implemented. Once the state implemented the Enterprise Architecture process, ITD rolled the relevant standards into

Enterprise Architecture where they became IT standards and then discontinued the Security and Internal Control Framework. ITD does not have any other formal security plan.

Enterprise Architecture developed a comprehensive list of security IT standards for the state.

All security requests are processed through ITD's Work Management System. Agencies prepare work orders and attach the appropriate security service requests to the work order and submit it to ITD. ITD retains the work orders in the Work Management System for an audit trail.

ITD developed a system for security logs on all systems where ITD is responsible for the login process. This system extracts security incidents and e-mails the details to the responsible agencies.

Finding: ITD lacks a formal Security Plan

Security plans are needed to provide centralized direction and control over information security. The lack of a formal security plan increases the risk that information security will not be consistently applied across the organization and increases the dependence on the expertise of current employees.

Recommendation

We recommend that ITD develop a security plan that provides centralized direction and control over information security.

ITD Response

ITD agrees with the recommendation and will develop a formal security plan. While ITD does have dedicated security staff that focus on enterprise security issues and procedures, we do agree that there is value in formalizing existing processes and standards into an overall plan.

Work Done by Consultant

In addition to the work above we hired a consultant to perform a security assessment of the State network. The following information is taken from the consultant's work.

External Security Assessment

An External Security Assessment is intended to provide an organization a snapshot of the overall security and risk picture of the network from an external (Internet) point-of-view. External Security Assessment procedures focus on performing extensive Internet research, discovering systems connected to the Internet and selectively probing these systems to discover misconfigurations and vulnerabilities. Additionally, External Assessments provide a means to capture the responsiveness of an organization's security devices and personnel. The External Security Assessment was a "zero knowledge" assessment in which the Test Team had no previous knowledge of the State's network. The assessment approach presented here consists of passive and active mapping and vulnerability analysis.

Internal Security Assessment

An Internal Security Assessment is intended to provide an organization with a snapshot of the overall security and risk picture of the systems and network under assessment. Internal assessment procedures focus on examining networked systems for known vulnerabilities, misconfigurations, and implementation flaws that may expose the system to additional risk and is comprised mostly of automated testing complimented by manual inspection.

A vulnerability assessment provides an organization the opportunity to correct deficiencies. These are likely to include missing patches or updates, superfluous services, weak passwords, and violations of the principle of least privilege.

This assessment includes an enumeration of systems and services, obtained using scanning tools. This type of enumeration also includes scanning for account information, including usernames, email addresses, passwords, and account policies. The tools and techniques used are not disruptive in nature and are designed not to negatively impact network operations. Information to be collected in this phase includes, but is not limited to:

- Service banners
- Open network ports
- System accounts and passwords
- Name services, directory services, web services
- Trust relationships

This enumeration was confined to internal networks as identified by the State of North Dakota. Measures were employed to ensure that network components or platforms outside of this limited range of servers were not scanned.

Vulnerability testing and identification is the process of employing tools and techniques in an attempt to verify potential vulnerabilities identified in the previous steps. Attempts will be made to circumvent or disable security controls in order to gain unauthorized access to a system or service. This process attempts to test all known vulnerabilities that potentially exist with the State's networks. It is important to emphasize the following with regard to vulnerability testing:

- Vulnerabilities often occur by exercising a system in a way that the developers had not considered.
- No known Denial of Service (DoS) tools or techniques were used in the vulnerability testing.
- No brute force password cracking was attempted.
- Occasionally unusual system configurations or states will behave in an unexpected way when tested. All attempts at mitigating impact to test systems were employed.

Finding: Excessive information is available regarding STAGENet

The Test Team was able to discover a large amount of information about the State of North Dakota's computer network, STAGENet, in a short amount of time. This is fairly typical of most large network infrastructures, and by itself does not present a serious risk to the security of the State's information.

Recommendation

We recommend that ITD limit the information available externally regarding STAGENet.

ITD Response

ITD agrees with the recommendation and is in the process of addressing the issues that allowed the security firm to access STAGENet documentation and standards from the external network.

Finding: Vulnerability scanning is not being done for all systems

ITD is responsible for configuring, deploying and maintaining a variety of systems providing services to state employees and the public. Other organizations such as state agencies and cities also configure and maintain systems which offer Internet services. ITD provides the Internet connectivity for these systems, and the traffic to/from these systems traverses ITD

maintained firewalls. ITD however, does not control these systems and can not ensure they are properly configured and patched. ITD Security performs regular vulnerability scans of ITD systems which provide services to the Internet, but does not scan systems used by other state agencies.

As a result, ITD Security can not fully evaluate or control the state's external security posture. Systems with vulnerabilities should be documented, evaluated and a determination made as to the validity of the vulnerability. For vulnerabilities determined to be valid, corrective action should be required and implemented (e.g. apply patch or other mitigation)

Recommendation

We recommend that ITD extend vulnerability scanning to all state systems which provide services to the internet.

ITD Response

ITD agrees with the recommendation. ITD's security staff already scans other state agency systems when requested by the agency. We will modify our processes to include regular scans of state agency systems and coordinate the resolution of any identified security risks.

Finding: Multiple, sometimes insecure, remote management solutions are in use

During the Internal Assessment, various remote management applications for Windows systems were noted. Some of these applications do not require or utilize encryption and as a result these systems are vulnerable to sniffing.

Recommendation

We recommend that ITD establish a policy for remote management of Windows systems which mandates the use of a single solution providing for the encryption of usernames/passwords and all session data.

ITD Response

ITD understands the logic behind this recommendation and will evaluate simplifying the number of solutions used to remotely manage Windows systems. ITD agrees that regardless of the solution or solutions, encryption of usernames and associated passwords should occur which is consistent with current Enterprise Architecture standards. In addition, there are security advantages to encrypting the session data as well and ITD will consider this criterion in deploying our remote management solutions.

Finding: Lack of a formal incident response program

ITD does not have an incident response (IR) program in place. There is a draft procedure in development, but ITD currently lacks a formal IR process. This process should include reporting requirements with Points-of-Contact (POC) to ensure proper and timely notification. The process should also include initial steps to be followed by the owning agency and responsibilities of ITD Security. It is recommended ITD Security be the focal point for all state IR and empowered to determine the continued operational status of the system(s) in question and course of action based on the accessed risk. The IR program should also include the ability to perform advanced host and network based forensics either by ITD or by a qualified third party.

Recommendation

We recommend that ITD implement a formal incident response program.

ITD Response

ITD agrees with this recommendation. We already have a draft policy in place and will modify this to ensure that it addresses the issues noted above.

Finding: Firewall configurations out of date

ITD's firewalls have rules which no longer apply or are no longer in use. This includes hosts which are no longer on the network or hosts which no longer require connectivity.

Recommendation

We recommend that ITD review all firewall configurations to ensure the rules are necessary and applicable.

ITD Response

ITD agrees with this recommendation. We will include firewall configurations in our annual review of the security access granted by each agency.

Finding: IP and port filtering not used to limit access to critical systems

Many of the systems allow unrestricted access from the Internet. In some instances, applications allow access from any Internet user. Where possible IP-based access controls should also be implemented for state internet systems.

Recommendation

We recommend that ITD implement IP-based access controls for state internet systems.

ITD Response

ITD agrees with the overall concept behind this recommendation but chooses to mitigate this risk in multiple ways. While ITD has implemented some instances of IP-based access, this is not a practical control for the majority of the state's computing resources. ITD's current strategy is a combination of virtual private network (VPN) concentrators and dedicated security zones. Access to internal systems is controlled with VPN which restricts the computing resources a user may access. Additionally, those systems that require broader access for the public are put in separate security zones where additional security measures can be applied.

Conclusion

We conclude that ITD has met the objective of ensuring system security. The findings and recommendations noted are meant to improve the level of security offered by ITD and do not, in our view, represent significant issues that would affect the overall assessment of system security at ITD.

Objective – Managing Facilities

To provide a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards.

Controls

The Highway Patrol provides maintenance and security of the capitol complex, including the offices and facilities of ITD.

ITD's Security Officer supports the Highway Patrol administration procedures as specific to ITD.

ITD's off-site storage facility is physically secured through a combination vault door and cement walls and ceiling. There are no windows and only a small vent for air conditioning. There is a fire extinguisher located inside the off-site vault. There are no formal annual inspections; however, ITD personnel use the vault daily. ITD updates the vault combination upon every employee turnover, or annually at a minimum.

ITD's Computer Facility environmental controls include fire suppression, raised floors, water detectors, smoke alarms and air conditioning units. Semi-annual tests are done to verify correct alarm operation. Facility Management Division provides a UPS for back-up power and power regulation, and a generator for extended power loss. The UPS is tested semi-annually and the generator is tested weekly.

ITD's Computer Facility includes a separate agency server room where agencies can store their network / application servers. The servers are backed up and ITD assumes maintenance of the server operating system. Agency personnel may obtain limited access to the agency server room from ITD security personnel.

ITD's Computer Facility agency server room has a raised floor, smoke detectors, air conditioning, and security camera. Agency personnel are allowed access to the room through their key cards.

ITD's data center, network operations center, and second data center run off of UPS and have back up power generators

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's policies relating to facility management, physical security, safety, and fixed asset inventory.

We toured ITD facilities to ensure adequate protections were in place for physical security and environmental monitoring.

We reviewed the latest fire inspection report for ITD facilities.

We interviewed personnel responsible for operating the key card system regarding its function and also reviewed related policies and procedures.

We tested access rights for key ITD facilities.

We reviewed the UPS and backup generator to ensure they provided adequate protection from power loss.

ITD has a Physical Security Policy which covers access controls, vendor access, and escorting of visitors.

ITD does not have a written fixed asset inventory policy but in accordance with OMB policy ITD conducts a yearly inventory.

Our tour of ITD facilities found that the necessary protections from fire, water, humidity, and temperature are in place in the computer room. Facilities Management monitors, tests, and maintains the environmental sensors and alarms.

The backup facility is locked and contains humidity and temperature controls as well as fire detection. ITD monitors and logs temperature and humidity conditions daily.

The local fire department performs a yearly fire inspection of the entire capital building. They inspected ITD facilities in June and September of 2005. No significant problems with ITD facilities were noted in the inspection reports.

Facilities Management currently operates the key card system that protects ITD facilities. Operation of the key card system is being moved to Highway Patrol. ITD is responsible for issuing and recovering key cards with its employees. ITD controls access rights for the doors to its facilities. ITD's Physical Security Policy covers ITD's responsibilities with the key card system.

There are sensors in the UPS room to monitor the environment. Facilities Management uses the same monitor software to monitor this room as they use to monitor the computer room and the agency server room. If the room gets too hot, the UPS shuts down and transfers the load to MDU. The system issues a high temperature warning at 78°F and shuts down the system at 85°F. The UPS and batteries are tested twice per year, generally in May and November.

Conclusion

We conclude that ITD has met the objective of managing facilities.

Objective – Managing Operations

To ensure that important IT support functions are performed regularly and in an orderly fashion.

Controls

ITD's computer operations include instructions for operators such as checklists, IPL instructions, shut down procedures, restart procedures, on-call lists, console commands, and other miscellaneous memos.

ITD uses Operations Planning and Control Scheduler (OPC) to schedule nightly jobs on the mainframe. Production control employees or agency personnel can schedule jobs in OPC. Production control specialists review the nightly job schedules. Jobs that abend (abnormally end) will send a message to the mainframe master console. Operators will then contact on call programmers and responsible agency personnel to fix the job.

ITD computer operations utilize IBM's Syslog (System Log) to log activity on the mainframe.

ITD's Computer Operations and Production Control teams ensure operations are adequately managed by maintaining and/or following documented operational instructions, managing and evaluating performance statistics over hardware and peripheral capacity utilization and performance, ensuring equipment is maintained on schedule, and ensuring a physical and logical segregation of source and object, test / development / production libraries.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding operations shifts and shift rotation procedures.

We reviewed the job scheduling software used on the mainframe.

We reviewed the operations checklists, IPL instructions, shut down procedures, and job restart procedures.

The operations staff has established regular business hours. If operations receives a call outside of these regular hours, an automated voice response system notifies the on-call person. ITD schedules two employees for each shift so if someone is absent, they still have someone available.

OPC is a mainframe product that schedules all jobs. Two employees run the OPC environment. The two employees do all the scheduling and changes to jobs except for the Bank of North Dakota and the Tax Department, who are responsible for their own jobs. These two employees also coordinate the scheduling of interdependencies among jobs. The operations staff ensures that the jobs run and uses OPC to recover from job aborts.

The shut down procedures and job restart procedures are included in the IPL instructions. The IPL instructions were found in the operations room.

Conclusion

We conclude that ITD has met the objective of managing operations.

Objective – Ensure Compliance with External Requirements

To meet legal, regulatory and contractual obligations.

Controls

ITD manages its legal and contractual responsibilities and liabilities through ongoing internal monitoring of legislation, contracts, and regulatory changes.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD identifies external requirements and ensures compliance with them.

ITD identifies external requirements in two ways. For large projects or legislation that ITD is directly involved in, ITD is aware of these by their very nature. For legislation or contracts that other agencies are involved in the creation of, ITD becomes aware of these external requirements usually when the agency notifies ITD.

To ensure compliance with external requirements, ITD normally delegates the responsibility to the division director most affected by the requirements.

Conclusion

We conclude that ITD has met the objective of ensuring compliance with external requirements.

Objective – Managing Performance and Capacity

To ensure that adequate capacity is available and that best and optimal use is made of it to meet required performance needs.

Controls

ITD schedules mainframe / mid-tier operating system down-time with agency IT coordinators, posts the outage schedule on the website, and provides web-based subscription service for automated email notifications of future scheduled maintenance activities.

ITD monitors computer and network operations performance based on assessments of individual systems and the knowledge of support and project teams, tools such as graphs, operator's knowledge, and available performance capacity system software. Performance management reports include e-mail messages by platform for e-mail servers, CPU utilization, DASD I/O per second, memory pages per second, and disk capacity for the mainframe.

ITD's mainframe and AS/400 platforms include redundant hardware controls to ensure continued operations in event of a part failure, and the mainframe O/S software will contact IBM technical service support as necessary.

ITD has implemented Mercury SiteScope infrastructure monitoring software over the state network platform to monitor performance characteristics (utilization, response time, usage and resource availability). ITD has configured SiteScope to automatically detect and report/record incidents over network resources.

ITD's Computer Systems Division utilizes HEAT incident tracking system to address issues - escalation procedures are being followed and appropriate in resolving problems.

ITD's Computer Systems Division has implemented ongoing procedures to monitor performance and capacity of the mainframe and mid-tier operating systems within the computer facility, and maintains historical statistics for future capacity planning and budgetary planning purposes.

ITD critical servers have redundant power supplies and all disk systems utilize RAID to ensure no data loss due to hard drive failures.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD monitors performance and capacity.

We interviewed ITD personnel regarding how ITD addresses the availability of systems and ensures fault tolerance for critical systems.

We reviewed the results of the most recent performance and capacity evaluation.

ITD uses Enterprise SiteScope to monitor the performance of critical systems. SiteScope monitors systems by periodically pinging them to determine if they are "alive". SiteScope also checks periodically to determine if applications are running. If SiteScope finds that the network or an application is down, it triggers an email, text message, or phone call (depending on the criticality of it) to the appropriate person. On the mainframe and AS/400, SiteScope only pings them. SiteScope does not check for applications that are still running on the mainframe or AS/400 because they have their own tools that do this.

For email ITD does capacity planning by keeping track of the number of email users and accounts. For the mainframe and the AS/400, they track things such as disk utilization and processor performance and chart these numbers over the course of several months. There are also spreadsheets that show the available disk space on servers.

The mainframe and AS/400 are on maintenance contracts. They have ETL (Extract, Transform, and Load) lines that contact IBM if a part fails in those boxes. It automatically orders the part/s that it needs and notifies the two IBM systems engineers in Bismarck. The two employees have full access to the facilities to fix any problems that occur.

We reviewed a file that showed outage avoidance statistics. This file showed planned and unplanned outages on certain systems, along with what the outage was for, whether there was any data loss or service interruption, and how long the outage was. We also reviewed their capacity planning evaluation for the mainframe and AS/400.

Conclusion

We conclude that ITD has met the objective of managing performance and capacity.

Objective – Assist and Advise Customers

To ensure that any problem experienced by the user is appropriately resolved.

Controls

ITD's Customer Service Division Support Center operates a help desk and provides a full-service central repository for customers to report problems, ask questions, request information, and receive back resolutions and answers in an organized and expedient manner.

"ITD's Support Center receives requests via telephone and email, and logs / tracks the requests through HEAT from FrontRange Solutions - Incident Management System. ITD has implemented HEAT with the following control parameters:

- Defined assignment groups, supervisors, and role-specific security
- Defined incident categories, call-types, sub-call-types, and incident priority matrix
- Defined detail screens to gather call-type specific information, and customer-specific details
- Acknowledgement, escalation, and communication procedures
- Monthly reporting & analysis, incident records archived 3 years"

ITD's Customer Service Division performs monthly reporting and analysis of incident records (HEAT) and Automatic Call Distribution (ACD) telephone system records, and tracks performance measures based upon key indicators.

ITD's Customer Service Division has implemented the Continuous Improvement Cycle based upon IT Infrastructure Library (ITIL) best practices for Service Desks, Incident Management, and Change Management.

ITD's Customer Service Division staff including the Customer Service Director, Service Center Manager, one full-time Service Management Software Analyst and five full-time Service Desk Analysts. Service Desk Analysts cover 7am - 5pm M-F and rotate on-call Saturday morning through Monday 7am. Computer Operations staff cover calls 5pm - 7am M-F.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding the registration of queries, escalation of those queries, and how queries are monitored and cleared.

We reviewed Help Desk policies and procedures.

We reviewed the latest performance measures for the Help Desk.

All customer queries are logged on a product called HEAT, a FrontRange product. Every call is logged, prioritized, and then assigned to an ITD group. ITD has a 15 minute standard during which the assigned group is to acknowledge that they received the ticket and that they agree that it should be with their group. That group then passes it on to an individual who resolves it. Once a group takes responsibility for a ticket, they can escalate it within their group if they choose. Throughout this process, the incident stays open in the system. The software allows the technician to add notes to a ticket. The software also updates the customer of the status of the incident. When ITD resolves the incident, ITD adds the resolution to the ticket, and closes it. At this time, a follow-up survey is sent to the customer.

ITD uses two priorities for HEAT tickets – priority one and priority three. Priority one means some core business functionality is lost. All others would be classified as a priority three. ITD starts working on priority one tickets as soon as they receive the ticket, and they work on it until they resolve it. They work on it 24 hours a day, seven days a week, or until they reach a point where the ITD and the customer agree to stop their efforts at resolving the problem.

SiteScope, a software monitoring product, monitors systems constantly. If the software finds a problem, it triggers a HEAT ticket automatically.

Help Desk policies and procedures contain contact information to reach employees after hours in case of emergency, a HEAT assignment guide which shows the ITD group to send HEAT tickets to for particular problems, and an on-call rotation schedule, along with procedures for determining daily rotation duties.

ITD sends out a yearly customer survey that spans all ITD divisions, including the Customer Service Division. We reviewed the results of the survey that was done in 2005. The results are in a chart, showing last years rankings in comparison with the previous 7 years. The four areas measured were professionalism & courtesy, availability, time to acknowledge, and time to resolve. The support center had favorable scores.

Conclusion

We conclude that ITD has met the objective of assisting and advising customers.

Objective – Define Information Architecture

To optimize the organization of the information systems.

Controls

All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business results or the business use of the object. There is one and only one owner for each object - the owning agency appoints an agency security officer who is responsible for controlling access rights.

ITD has established an Enterprise Architecture process. This process relies on participation of agency representatives. Each agency that is interested is invited to participate in various domain teams that study specific technology domains and provide proposals to the Architecture Review Board (ARB) and State Information Technology Advisory Committee (SITAC). This process addresses enterprise technology issues and results in state standards, policies and guidelines.

A Compliance with Standards section is included in agency IT plans. Agencies indicate the status of their compliance with standards and policies and if not in compliance, provide an approved waiver request and provide plans to bring the agency into compliance.

ITD is legislatively mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. The Enterprise Architecture (EA) process promotes state agency participation with ITD in setting future direction of information technology in the state of North Dakota.

ITD's policies and procedures address the classification of data, including security categories and data ownership, and access rules for the classes of data are clearly defined.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding data ownership.

We reviewed ITD's data ownership policies and procedures

ITD Mainframe Computer Security Policy defines the owner as the agency responsible for the business results of the object, and there can be only one owner per object. The owning agency has a security officer designated by the agency's director. The designation must be made in writing.

ITD does not classify data by security categories.

Conclusion

We conclude that ITD has met the objective of defining the information architecture.

Objective – Determine Technological Direction

To take advantage of available and emerging technology to drive and make possible the business strategy.

Controls

ITD maintains a biennial Strategic Business Plan, outlining goals and objectives for each division, and follows a methodology for measuring progress toward the goals outlined in the business plan, per NDCC 54-59-06.

ITD has established an Enterprise Architecture process. This process relies on participation of agency representatives. Each agency that is interested is invited to participate in various domain teams that study specific technology domains and provide proposals to the Architecture Review Board (ARB) and State Information Technology Advisory Committee (SITAC). This process addresses enterprise technology issues and results in state standards, policies and guidelines.

A Compliance with Standards section is included in agency IT plans. Agencies indicate the status of their compliance with standards and policies and if not in compliance, provide an approved waiver request and provide plans to bring the agency into compliance.

ITD is legislatively mandated to develop policies, standards, and guidelines for technology based on information from state agencies, institutions, and departments with the goal of creating a common statewide architecture. The Enterprise Architecture (EA) process promotes state agency participation with ITD in setting future direction of information technology in the state of North Dakota.

ITD's technological infrastructure is maintained on an ongoing basis, takes into account current and future technology trends and regulatory conditions, and is compared with the IT long and short range plans.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed the infrastructure plan within ITD's Strategic Business Plan.

We interviewed ITD personnel regarding how the infrastructure plan is developed.

We reviewed the IT standards related to infrastructure.

ITD's Strategic Business Plan broadly states some principles, objectives, and goals that affect infrastructure:

- ITD will cost effectively invest in technology.
- ITD will provide vision and direction for IT investments in North Dakota government.
- ITD will be the preferred provider of strategic IT services for government and education.

ITD does not maintain a formal plan specific to technological infrastructure. Rather ITD addresses infrastructure in two ways. The first way is a project-driven approach. Certain projects require ITD to address infrastructure issues. These issues are analyzed and addressed during the project management/oversight process.

The second approach is through the Strategic Business Plan. The Strategic Business Plan states certain goals, objectives, and principles that affect ITD's plans for infrastructure. The

infrastructure plans are further elaborated upon in certain division-level documents that are related to the Strategic Business Plan.

We reviewed the IT standards related to infrastructure, and conclude that the standards are in agreement with ITD's Strategic Plan. The standards help enforce ITD's goal of setting a vision and direction for IT investments and incorporate ITD's concern for cost effective IT solutions.

Conclusion

We conclude that ITD has met the objective of determining technological direction.

Objective – Define IT Organization and Relationships

To deliver the right IT services.

Controls

ITD Organizational Structure - divided into seven divisions (Administrative Services, Software Development, Computer Systems, Telecommunications, Customer Service, Human Resources, IT Planning) to ensure authority and independence from user organizations.

ITD publishes a quarterly agency newsletter titled "Information Link." ITD also coordinates the "IT Directional Meeting" for executive branch agency representatives to inform them on current initiatives and issues.

Per NDCC 54-59-07, the Statewide Information Technology Advisory Committee (SITAC) advises ITD regarding statewide IT planning, including providing e-government services for citizens and businesses, developing technology infrastructure to support economic development and workforce training, and developing other statewide IT initiatives and policy.

ITD's Administrative Services Division has formally assigned to a security officer organization wide responsibility for formulation of internal control and security (logical and physical) policies and procedures.

ITD's Human Resources Division has established policies and procedures for the evaluation and re-evaluation of IT position descriptions.

Governance structures are in place to set the direction over the enterprise programs, CJIS, ConnectND, and GIS.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed the enabling legislation for ITD.

We reviewed the enabling legislation for the Statewide Information Technology Advisory Committee.

We reviewed an organizational chart for ITD.

We reviewed the job description for the ITD security officer.

The 1999 legislature passed legislation to create the Information Technology Department (ITD) and transition all responsibilities from the former Information Services Division (ISD) to the newly created Information Technology Division. ITD is an internal service organization that provides services to other government agencies for a service charge. North Dakota Century Code § 54-59-01 defines the duties and responsibilities of ITD. The Chief Information Officer reports directly to the governor.

The 2001 legislature passed legislation that created the State Information Technology Advisory Committee (SITAC). North Dakota Century Code § 54-59-07 defines the duties of SITAC as "The committee shall advise the department regarding statewide information technology planning, including providing electronic government services for citizens and businesses, developing technology infrastructure to support economic development and work force training, and developing other statewide information technology initiatives and policy."

ITD is organized into seven divisions. Each division is clearly defined.

The Security Officer job description clearly states that the position is responsible for establishing security policies and standards and administering security systems for following platforms: "mainframe, mid-range, PC's, servers, databases, firewalls, dial-up, Virtual Private Network (VPN), digital certificates, anti-virus, and physical security."

Conclusion

We conclude that ITD has met the objective of defining the IT organization and relationships.

Objective – Manage the IT Investment

To ensure funding and to control disbursement of financial resources.

Controls

The governor and state legislature set staffing levels biennially in ITD's budget. During the biennial budget process, ITD reviews staffing levels and requests additional FTE as needed.

ITD rate setting process and annual report include comparisons to similar rates charged by other states and private sector providers to ensure that the rates are competitive with similar services offered by other states and the private sector.

ITD establishes the operating budget through the executive planning process (Budget Analysis & Reporting System) and manages budget v. actual expenditures through the centralized PeopleSoft accounting system. The budget is aligned with the enterprise strategic plan. Executive Branch agencies participate in preparing their portions of the IT plan. A goal of the process is to anticipate major infrastructure needs and plan accordingly.

ITD's annual report includes: benefits realized from investment in technology; a status report on large and small projects; ITD's performance against goals: ITD's service rates (20 rates that generate 90% of ITD revenue) which are compared with costs charged by similar organizations; the strategic planning process; an update on internal performance measures, and future IT initiatives. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee. The report is also available at ITD's website under "Publications".

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's appropriations bill for the 2005-2007 biennium

We reviewed ITD's Annual Report.

We interviewed ITD personnel regarding how ITD develops and submits their budget request.

The explanations for changes in budget from the previous biennium contained in the Executive Budget Recommendation and the Final Legislative Budget appear to be adequate and the dollar amounts of the changes appear to be within reason given the explanation.

ITD includes a comparison of rates within their annual report. ITD explains that rates are charged to mainly cover costs. Rates are compared to other entities mainly in an effort to ensure that quality services are provided at a fair price. ITD provides a comparison of rates for twenty of its services. The rates are always compared to other states in the region and are also compared to the rates of third-party vendors where applicable.

In January of the even-numbered years, ITD begins their budget preparation process. In January through February, ITD performs preliminary rate reviews which are a comprehensive review of the rates that is also focused on anticipating what the rates will need to be in the coming biennium. The preliminary rate review results in the draft rates for the coming biennium. These draft rates enable agencies to complete their IT plan with a reasonable idea of what to expect to pay for ITD services. In March and April, the ITD's division directors begin planning for expenditures that focus more on ITD's strategic plan rather than the regular operating

expenditures. Such expenditures associated with updating or expansion of architecture and infrastructure or projects focused on improving ITD services are analyzed. In April, ITD reviews its expenditures for the first year of the biennium and uses this information to create finalized rates which agencies can use in planning their budgets. In June, July, and August, ITD reviews agency IT plans to develop the statewide IT plan. The various projects proposed by other agencies are reviewed to determine the affect they have on ITD's own budget. ITD determines if the projects change the architecture and infrastructure plans, if more FTE will be needed, or if more money will be needed for consultants. The budget is then completed in August or September.

Conclusion

We conclude that ITD has met the objective of managing the IT investment.

Objective – Communicate Management Aims and Direction

To ensure user awareness and understanding of those aims.

Controls

ITD policies and procedures are published and made available to ITD employees on the intranet.

ITD management and staff meet on a scheduled basis to discuss internal operations and direction. Division meetings are held monthly, management and supervisors meet weekly, and all ITD staff meets twice per year.

ITD organizational controls ensure appropriate and adequate resources are assigned to implement the organization's policies in a timely manner.

ITD procedures exist to address the need to periodically review and approve key standards, directives, policies and procedures relating to information technology.

ITD's security and internal control framework specifies the internal control policy, purpose and objectives, management structure, scope within the organization, assignment of responsibilities, and definition of penalties and disciplinary actions associated with noncompliance.

ITD's policies and procedures define, document, and maintain a formal philosophy, policies and objectives governing quality of systems and services provided by the organization.

ITD management promotes a positive control environment by example and has accepted full responsibility for formulating, developing, documenting, promulgating, controlling and regularly reviewing policies governing general aims and directives.

ITD evaluates the internal control processes within the department on an ongoing basis, through management meetings, budgetary review, external audits - including SAS70 reviews, internal security assessment, and through internal assessment of policies and procedures.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD develops and maintains their policy manual and how they ensure adequate resources are assigned to implement the policies.

We reviewed ITD's policy manual.

We reviewed minutes from ITD's meetings with employees to determine if they communicate and train staff regarding the control environment.

Potential policy and procedures manual changes can come from issues raised at staff meetings, exit interviews, employee surveys, and through a formal process where changes are submitted to human resources. The Employee Policy Council, made up of the directors and some human resources personnel, meets quarterly to specifically discuss potential policy changes. Policy changes are approved by this council. If the council approves the changes, they update the manual, and send an e-mail to ITD staff informing them of the changes made to the manual. The policy and procedure manual is kept on ITD's intranet.

The policy manual was last updated July 1, 2004. The manual includes policies addressing integrity, ethical values, code of conduct, security and internal controls, competence of personnel, and management philosophy and operating style. Policies relating to quality of services are mentioned as part of the mission and vision and are mentioned briefly in the general rules of conduct. For most policies, the reason for the policy is detailed. The policy manual also explains the different types of disciplinary actions that may be taken and when those actions should be used.

In the Policy Committee Meetings, nothing was on the agenda for any of the 2005 meetings that concerned the control environment.

In the Semi-Annual Staff Meetings, the confidentiality of agency data was emphasized each time. There was also mention of the standardization of personal computers and how that would benefit security. There were no other items related to the control environment and security.

During the Weekly Management Meetings for the month of April 2005, one control issue was brought forth (acceptable use of the internet).

Conclusion

We conclude that ITD has met the objective of communicating management aims and direction.

Objective – Assess Risks

To support management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors.

Controls

ITD's Contingency Planning Specialist is responsible for establishing and maintaining ITD's disaster recovery plan through participation in the Continuum of Government Team, formed in June 2002, headed by the Office of Management and Budget - Risk Management Division. This team is tasked with establishing a uniform web-enabled relational database software application from Strohl Systems Group, Inc. - Living Disaster Recovery Planning System (LDRPS).

ITD maintains a consistent philosophy and framework over business contingency plan development and prioritizes internal and statewide applications with respect to criticality and timeliness of recovery, as mandated by the Continuum of Government Team, through criteria listed in the LDRPS system.

ITD manages risks associated with individual procurement contracts based on the dollar value and by requiring agencies to provide documented requests for information technology.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's disaster recovery plan for risk assessment documentation.

We interviewed ITD personnel regarding how ITD assesses risks, responds to risk identified, and updates the risk assessment over time.

ITD considers IT risks in an ad hoc manner. In the areas of security and disaster recovery ITD has developed good processes and controls that suggests that a risk assessment was done, however; the risk assessment was not documented.

Finding: ITD lacks a formal risk assessment framework

While critical business processes have been identified, there is not a systematic approach to identifying, assessing, and mitigating or accepting risks to those business processes. Such a framework should incorporate a regular assessment of the relevant information risks to the achievement of the business objectives, forming a basis for determining how the risks should be managed to an acceptable level. Management should ensure that reassessments occur and that risk assessment information is updated with results of audits, inspections and identified incidents. Without a formal risk assessment process management may not have adequate information to make sound decisions in the use of assets to mitigate risks.

Recommendation

We recommend the Information Technology Department develop a systematic risk assessment framework.

ITD Response

ITD agrees with the recommendation and will leverage our relationships with other security organizations in other states to determine best practices in this area.

Conclusion

We conclude that, except as noted above that risk assessments are done in an ad hoc manner, ITD has met the objective of assessing risks.

Objective – Managing Projects

To set priorities and to deliver on time and within budget.

Controls

North Dakota Century Code Section 54-35-15.2 provides that the Legislative Information Technology Committee shall “review the cost-benefit analysis of any major information technology project (=> 250K per biennium or => \$500K in total) of an executive or judicial branch agency” and “perform periodic reviews to ensure that a major information technology project is on its projected schedule and within its cost projections.”

ITD's large project reporting has five phases: business case, project plan, quarterly status reports, summary status report, and post-project analysis. In the business case phase the agency defines the business requirements, does a cost/benefit and risk analysis, establishes a project manager and executive steering team, and presents this to the Legislative Information Technology Committee. ITD has established guidelines for making the business case. The project plan is to be prepared based on industry “best practices.” ITD encourages the use of the Project Management Institute (PMI) format. Quarterly reports define the scope of the project and state the project schedule. The report compares budgeted to actual costs and outlines current progress and issues. ITD's planning analysts review the report and present summary status reports to the Legislative Information Technology Committee each quarter. The post-project analysis assesses whether the project accomplished its business objectives.

ITD's large project oversight process ensures the project plan includes a formal system development life cycle for system development and installation, including requirements definition, coding, testing, conversion, training, and documentation.

ITD's large project oversight process incorporates quality management processes within the project plan.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's project management and large project guidelines.

We interviewed ITD personnel regarding how ITD monitors large projects.

We reviewed the latest large project status report.

The ND Project Management Guidebook was created to provide a common methodology for managing projects within state government. This guidebook is to be used not only for in-house projects, but also for private vendors that desire to participate in a state project. Each phase lists and describes the key processes, roles, and deliverables associated with that phase. Each phase also lists frequently asked questions and common pitfalls and how to avoid those pitfalls.

The Large Project Oversight website describes what a large project is and refers to the ITD Standard and statutory requirements that affect large projects. The website provides many other resources to those involved in a large project. These resources include the Guidebook and an overview of the large project reporting process. Also included are several templates for reports as well as links to reports completed by previous large projects.

When a new large project is proposed, a business case must be submitted to ITD. ITD reviews the business plan to ensure that is complete (includes cost/benefit analysis, project risks, project description and objectives, and description of how project is consistent with the agency's mission). Once the business plan is finalized, it is submitted to the Legislative Council. ITD obtains the project charter after it has been approved by the project sponsor. After the project charter is accepted, an Executive Steering Committee is created to help support the management of the project. The Executive Steering Committee includes an ITD analyst as a member. The Executive Steering Committee meets quarterly to review the projects status and provide guidance to the project manager. Once the project plan is approved by the project sponsor, a copy is sent to ITD.

On a quarterly basis, a project status report, the current version of the project plan, and the project performance assessment must be submitted to ITD. ITD uses these submissions to create the Large Summary Project Report which is submitted quarterly to the Legislative Council.

Upon completion of the project, the agency completes a Post Implementation Review and submits it to ITD. ITD reviews and accepts the review and then passes it along to the Legislative Council.

Our review of the most recent project status report showed that the projects were on track and ITD was adequately monitoring them.

Conclusion

We conclude that ITD has met the objective of managing projects.

Objective – Install and Accredit Systems

To verify and confirm that the solution is fit for the intended purpose.

Controls

ITD utilizes separate test and production environments for critical systems. Some systems have separate development environments as well. New applications or application changes are tested by users in the separate test platform or region. After acceptance ITD system administrators and or DBA's migrate the changes to production.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding the process for migrating agency purchased applications to the shared production environments.

ITD works with the vendor of the application and the agency to identify what the resource requirements. They determine if multiple applications on one server will co-exist with each other. ITD looks at the usage patterns of the applications when determining which applications will share a server. They look to see if the applications use a lot of resources at certain time periods and try to pair up the applications accordingly. They also talk to the vendor about security requirements. They determine what type of access is needed and how the application interacts with the server.

All applications are put in the test environment just to make sure that there are no undocumented features in the application. They do load testing on all web applications to make sure performance requirements are met. They build a temporary test server for testing a unique application. They will also load any applications onto the test server that will co-exist with the application in the production server. After ITD installs the application into the test environment and does their testing, they then hand it over to the agency. The agency then does their testing on the applications making sure it is functioning like it should. The agency is then required to submit a work request through the Work Management System (WMS) for the migration of an application from the test environment to the production environment. The agency's WMS request indicates to ITD that the agency's testing has been successfully completed. ITD then moves it into production. The test environment goes away after the application is moved into production. Any major upgrades for the application go through the same procedures of testing as they do when the application is new.

Conclusion

We conclude that ITD has met the objective of installing and accrediting systems.

Objective – Manage Changes

To minimize the likelihood of disruption, unauthorized alterations, and errors.

Controls

ITD Distributed Systems utilizes a web-based change management system to log changes. Changes are logged in the system and approved by the Computer Systems Manager or the System Architect.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD tracks and authorizes changes.

The majority of change requests are initiated by the end user through ITD's Work Management System. ITD is beginning to develop and formalize a change management process. During CY05, ITD implemented a simple web-based change management application that is backed by an SQL database. System administrators can access the application to request a change. The application records the User ID of the requestor and the time and date of the request automatically. The requestor must fill in a title for the change request, the category of the change, the date the change needs to be made by, and a detailed description of the change. When this is submitted, an e-mail is sent to Computer Systems Manager to notify them of the change request. The Computer Systems Manager then must access the application and approve or deny the change request.

Conclusion

We conclude that ITD has met the objective of managing changes.

Objective – Identify and Allocate Costs

To ensure a correct awareness of the costs attributable to IT services.

Controls

ITD sets its rates to cover the cost of providing services with a reasonable surplus to finance capital purchases. ITD monitors actual expenditures to billings through the PeopleSoft accounting system cost centers (overhead, systems, programming, telecommunications, IBM central computer, AS/400 computer, micrographic, direct billing, basic phone, in-state long distance, out-of-state long distance, direct billing, and relay service) with the goal of matching billings to expenditures within each cost center.

ITD's strategic planning process outlines the rates and funding mechanisms necessary to finance the proposed activities of the department, in accordance with NDCC 54-59-06.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding how ITD sets rates.

We reviewed ITD's Strategic Business Plan for rate information.

We selected five rates and tested whether they covered the costs with a reasonable surplus to finance capital purchases.

In January of every even-numbered year, ITD begins to set rates. They have primary cost centers that correspond to the primary services they offer. They do different scenarios and projections to set the rates. The rates are generally published in March of the even-numbered years so agencies can prepare their budgets. In setting these rates, ITD makes some "best guesses" as to things such as future compensation, trying to ensure they don't have to go back and adjust rates after agencies have already set their budget.

ITD also does financial statement and analytical review every month. Every month, they prepare a cost center statement that shows how each cost center is performing. They look at what the trend is for each cost center, whether it is over-recovering and under-recovering. They also prepare a cash flow projection where they look at any large payments that need to be made in the future.

In ITD's 2005-2007 Strategic Plan, one of their financial goals is to manage revenue sources to cover costs and to ensure competition and stable rates. There are two objectives for this goal. The first objective is to charge competitive rates for comparable services, while maintaining the appropriate operating reserve. The second objective is to develop budget rates for each biennium, and not exceed those rates for the biennium.

We tested the basic phone service, voice mail rate, device connection rate, VPN client, and Gold level disk storage rate. From our testing it appears ITD's rates are reasonable. They are set based upon the cost of providing the service, and take into consideration any large purchases that need to be made in the future.

Conclusion

We conclude that ITD has met the objective of identifying and allocating costs.

Objective – Managing Problems and Incidents

To ensure that problems and incidents are resolved, and the cause investigated to prevent any recurrence.

Controls

ITD's Customer Service Division Support Center operates a help desk and provides a full-service central repository for customers to report problems, ask questions, request information, and receive back resolutions and answers in an organized and expedient manner.

"ITD's Support Center receives requests via telephone and email, and logs / tracks the requests through HEAT from FrontRange Solutions - Incident Management System. ITD has implemented HEAT with the following control parameters:

- Defined assignment groups, supervisors, and role-specific security
- Defined incident categories, call-types, sub-call-types, and incident priority matrix
- Defined detail screens to gather call-type specific information, and customer-specific details
- Acknowledgement, escalation, and communication procedures
- Monthly reporting & analysis, incident records archived 3 years"

ITD's Customer Service Center has implemented the Continuous Improvement Cycle based upon IT Infrastructure Library (ITIL) best practices for Service Desks, Incident Management, and Change Management.

Tests of Operating Effectiveness and the Results of Those Tests

We interviewed ITD personnel regarding their problem management procedures.

We interviewed ITD personnel regarding their emergency change procedures.

ITD's problem management is combined with incident management and logged using HEAT. ITD uses HEAT for problem management because they don't typically close an incident until they've discovered the underlying cause of it and solved the problem. They may let the customer know they have a work-around and they can be back up and running, but the ticket doesn't get closed until they find the underlying cause. Sometimes they close it and agree to monitor it or have the customer contact them if it happens again.

An incident is Priority 1 when some core business functionality is lost. For Priority 1 calls, the help desk operator makes a record in HEAT, and then makes verbal contact with the division in ITD they've assigned it to. They start working on the problem as soon as it's received and they work on it until it gets resolved, which may mean 24 hours a day, 7 days a week.

Conclusion

We conclude that ITD has met the objective of managing problems and incidents.

Objective – Define a Strategic Information Technology Plan

To strike an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment.

Controls

ITD maintains a biennial Strategic Business Plan, outlining goals and objectives for each division, and follows a methodology for measuring progress toward the goals outlined in the business plan, per NDCC 54-59-06.

ITD's Strategic Business Plan outlines goals and tactics for each division. Progress towards these goals and tactics is monitored on a quarterly basis by the Chief Information Officer and reported to the Legislative Information Technology Committee.

ITD's strategic planning process takes into account organizational changes, technology evolution, regulatory requirements, business process reengineering efforts and staffing requirements.

ITD meets with key customers on a monthly or quarterly basis to gather information about future plans and needs.

ITD's annual report includes: benefits realized from investment in technology; a status report on large and small projects; ITD's performance against goals: ITD's service rates (20 rates that generate 90% of ITD revenue) which are compared with costs charged by similar organizations; the strategic planning process; an update on internal performance measures, and future IT initiatives. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee. The report is also available at ITD's website under "Publications".

Per NDCC 54-59-07, the Statewide Information Technology Advisory Committee (SITAC) advises ITD regarding statewide IT planning, including providing e-government services for citizens and businesses, developing technology infrastructure to support economic development and workforce training, and developing other statewide IT initiatives and policy.

ITD conducts an annual customer survey to ensure the department is meeting customers' expectations. The survey allows customers to rate their satisfaction with the services provided by ITD and to suggestions for improvements. Survey areas are software development, computer services, E-mail services, support, telephone services, network service, records management, IT planning services, and an overall ITD survey. Results are published in ITD's strategic plan.

ITD evaluates progress toward the goals outlined in the strategic plan, and publishes the results in the annual report (balanced scorecard). ITD also tracks performance metrics internally, both at the department and division levels.

ITD provides guidelines for agencies to follow in preparing their technology plan, reviewing the plans for compliance with statewide policies or standards, resolving conflicting directions among plans, and assembling the agency plans into a statewide plan to be submitted to the members of the Legislative Assembly. ITD also reviews and approves technology acquisitions for conformance with the agency's IT plan and compliance with statewide policies and standards.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's most recent Strategic Business Plan and Annual Report.

We interviewed ITD personnel regarding how ITD sets goals and how they measure performance against them.

We reviewed minutes from the Statewide Information Technology Advisory Committee.

We interviewed ITD's personnel regarding meetings with key customers.

We reviewed the agency IT planning process which ITD oversees.

ITD prepares a biennial Strategic Business Plan and an Annual Report. The Strategic Business Plan outlines ITD's vision, goals, and objectives, the plan appeared to be consistent with the business goals of the State of North Dakota. The Annual Report measures ITD's performance but includes only selected performance measures. ITD meets monthly to discuss the Strategic Business Plan and progress towards objectives. ITD has assigned the responsibility to facilitate these monthly meetings to an individual.

The Statewide Information Technology Advisory Committee (SITAC) meets roughly quarterly and does provide advice on technology issues to ITD. The Chief Information Officer sets the agenda for SITAC meetings.

ITD personnel indicated that meetings with key customers occur. We reviewed agendas from past meetings; no minutes are kept from these meetings.

The duty for defining the form of biennial agency IT plans has been assigned to ITD. ITD has established guidelines for agency plans and has a process set up to assist agencies in their planning. ITD reviews finished plans for completeness and adherence to the guidelines.

Conclusion

We conclude that ITD has met the objective of defining a strategic information technology plan.