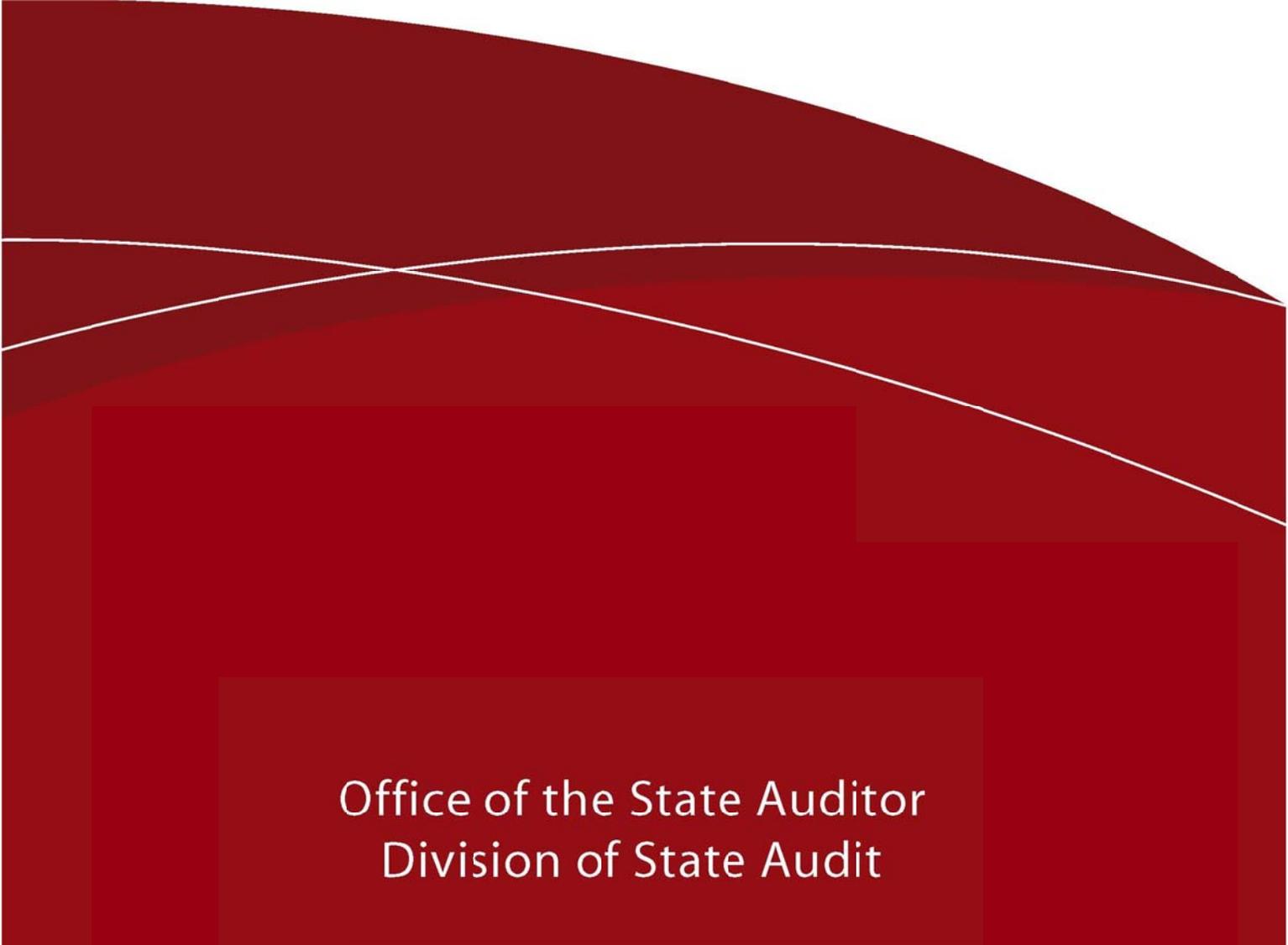




INFORMATION TECHNOLOGY
DEPARTMENT

Information System Audit

For the Fiscal Year ended June 30, 2010



Office of the State Auditor
Division of State Audit

Senator Randel Christmann – Chairman
Representative RaeAnn G. Kelsch – Vice Chairman

Representatives

Rick Berg
Merle Boucher
Jeff Delzer
Patrick R. Hatlestad
Jerry Kelsh
Keith Kempenich
Gary Kreidt
Louis Pinkerton
Chet Pollert
Bob Skarphol
Benjamin A. Vig
Lonny Winrich

Senators

Joan Heckaman
Jerry Klein
Judy Lee

TABLE OF CONTENTS

Executive Summary	2
Independent Auditor’s Report	3
Background Information	5
Objectives, Scope, and Methodology	8
Audit Scope.....	8
Audit Objectives	8
ITD’s Description of Controls	9
Overview of Operations	9
Control Environment	10
Management Control	10
Human Resource Control	11
Monitoring	12
Communication	12
Control Objectives and Related Controls.....	13
User Control Considerations.....	14
Information Provided by the State Auditor’s Office	15
Systems Development and Maintenance Controls.....	15
Logical and Physical Access Controls	16
Finding: ITD lacks a formal Security Plan.....	18
Finding: ITD lacks a formal risk assessment framework	19
Computer Operations.....	19
Subsequent Event Disclosure – Jan. 18, 2011 Power Failure	20
Incident Management Controls	22
Contingency Planning Controls	23

STATE AUDITOR
ROBERT R. PETERSON

Phone (701)328-2241
Fax (701)328-1406



STATE OF NORTH DAKOTA
OFFICE OF THE STATE AUDITOR
STATE CAPITOL
600 E. BOULEVARD AVENUE – DEPT 117
BISMARCK, NORTH DAKOTA 58505

January 21, 2011

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 June 30, 2010. 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 three 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,

A handwritten signature in cursive script that reads "Bob Peterson".

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 July 1, 2009 to June 30, 2010.

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.

Our audit resulted in the following significant findings:

- ITD lacks a formal Security Plan. (page 18)
- ITD lacks a formal risk assessment framework. (page 19)



STATE OF NORTH DAKOTA
OFFICE OF THE STATE AUDITOR
STATE CAPITOL
600 E. BOULEVARD AVENUE – DEPT 117
BISMARCK, NORTH DAKOTA 58505

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 June 30, 2010. The control objectives were specified by the management of ITD.

Our audit did not include vulnerability assessment or penetration testing as those objectives were performed under contract with an outside firm and that report was issued under separate cover.

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 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 June 30, 2010. 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 July 1, 2009 to June 30, 2010. 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 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.

A handwritten signature in cursive script, appearing to read "Bob Peterson".

Robert R. Peterson
State Auditor

January 21, 2011

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. The department may not exercise its powers and duties in a manner that competes or otherwise interferes with the provision of telecommunications service to a private, charitable, or nonprofit entity by a privately or cooperatively owned telecommunications company.”

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, software, or implementation services 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 five 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 or the legislative assembly before executing a financing agreement. If the budget section or the legislative assembly 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 seven and one-half percent of the amount appropriated to the department during that biennium.
5. Shall review requests for lease, purchase, or other contractual acquisition of information technology as required by this subsection. Each executive branch agency or institution, excluding 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.

6. 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.

7. Shall request and review information, including project startup information summarizing the project description, project objectives, business need or problem, cost-benefit analysis, and project risks and a project closeout information summarizing the project objectives achieved, project budget and schedule variances, and lessons learned, regarding any major information technology project of an executive branch agency, the state board of higher education, or any institution under the control of the state board of higher education as provided in section 54-35-15.2. The department shall present the information to the information technology committee on request of the committee.

8. May request and review information regarding any information technology project of an executive branch agency with a total cost of between one hundred thousand and two hundred fifty thousand dollars as determined necessary by the department. The department shall present the information to the information technology committee on request of the committee.

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

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

11. Shall collaborate with the state board of higher education on guidelines for reports to be provided by institutions under control of the state board of higher education on information technology in those entities.

12. Shall review the information technology management of executive branch agencies or institutions.

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

14. May provide wide area network services to a state agency, city, county, school district, or other political subdivision of this state. The information technology department may not provide wide area network service to any private, charitable, or nonprofit entity except the information technology department may continue to provide the wide area network service the department provided to the private, charitable, and nonprofit entities receiving services from the department on January 1, 2003. The department shall file with the state auditor before September 1, 2003, a description of the wide area network service the department provided to each private, charitable, and nonprofit entity receiving services from the department on January 1, 2003.

15. Shall assure proper measures for security, firewalls, and internet protocol addressing at the state's interface with other facilities.

16. Notwithstanding subsection 14, may provide wide area network services for a period not to exceed four years to an occupant of a technology park associated with an institution of higher education or to a business located in a business incubator associated with an institution of higher education.

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 July 1, 2009 to June 30, 2010. 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.

ITD'S DESCRIPTION OF CONTROLS

Overview of Operations

The Information Technology Department (ITD) is located in Bismarck, North Dakota. Pursuant to North Dakota Century Code (NDCC) chapter 54-59, ITD is managed by the Chief Information Officer who reports directly to the Governor. The department is responsible for all wide area network services planning, selection, implementation and operation for all state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, and school districts. ITD's responsibilities also include computer hosting services, software development services and statewide communications services for state agencies, universities, political subdivisions and schools. This description of controls addresses general controls related to the overall administration of the network and computing infrastructure used to host data and applications for the entities noted above.

ITD's mission is to provide leadership and knowledge to assist our customers in achieving their mission through the innovative use of information technology. In support of our mission ITD provides services to our customers through the following six divisions:

- The Customer Service Division serves as ITD's Single Point of Contact and assists customers in resolving issues. It connects customers with subject matter experts and works to simplify customer's business interactions with ITD. This division also coordinates with agencies on technology planning and enterprise initiatives.
- The Software Development Services Division develops and maintains computerized applications and provides related consulting services. Its responsibilities include design, development, and support of customized software applications that operate on a variety of computer platforms and database management systems. The staff is on-call to support production applications 24 hours per day. This division also has a staff of project managers available for assisting agencies on large IT projects.
- The Computer Services Division is responsible for central computer systems and their operations. The staff in this division oversees all architecture and system hardware to serve applications and world-wide-web based systems to state government agencies, political subdivisions and educational entities. Operations staff provides round-the-clock job processing and routine system procedures required during the non-business hours. The computer room is environmentally controlled and electrically protected by an uninterrupted power supply. All sections employ an on-call protocol to provide twenty-four hour support for system availability.
- The Telecommunication Services Division maintains telephone systems and services, video services and network infrastructure. The division designs and maintains the state's wide area network for all government and education entities in the state.
- The Administrative Services Division is responsible for fiscal administration, enterprise security administration, records management, micrographics, and contingency planning.
- The Human Resource Division is responsible for agency personnel recruitment and retention support to provide the right talent for the right job at the right time.

ITD has adopted six guiding principles to provide a set of values to guide employees in our daily operations and interactions with customers and vendors.

- Respect - we treat everyone with dignity and respect.
- Teamwork - we recognize ITD's success depends on partnerships and collaboration.
- Achievement - we develop quality solutions that best address the needs of our state. We are committed to delivering results on time and on budget.
- Integrity - we build long-term, lasting relationships through mutual trust. We value open, honest, two-way communication.
- Leadership - we encourage initiative and creativity. We are committed to investing in knowledge and expertise.
- Service - we hold ourselves accountable for a positive customer experience.

Control Environment

Management Control

ITD's Management Team is responsible for the overall control environment at ITD and for formulating, implementing and monitoring the controls in place in the various divisions of ITD. The management team consists of the Chief Information Officer, Director of Operations and the Directors of the six ITD divisions previously mentioned. This team meets on a weekly basis to discuss overall departmental projects, operational issues and progress towards departmental strategic goals.

The Management Team maintains a biennial Strategic Business Plan, outlining goals and objectives for the department, and follows a methodology for measuring progress toward the goals outlined in the business plan, per NDCC 54-59-06. After the plan is developed ITD evaluates progress toward the goals outlined in the strategic plan, and publishes the results in ITD's annual report. ITD also tracks performance metrics internally, both at the overall department and at the division levels.

ITD management and staff members meet on a regular basis to discuss internal operations and overall departmental direction. Within most divisions managers and supervisors meet weekly to discuss projects, operational issues and progress towards strategic goals. In addition to divisional meetings ITD holds an all ITD staff meeting twice per year to communicate with all employees about major initiatives, major policy changes and progress towards strategic objectives.

ITD establishes its biennial operating budget through the executive budget process utilizing the Office of Management and Budget's (OMB) Budget Analysis & Reporting System (BARS). 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 to ensure adequate staffing and technology resources are available for ITD services and projects.

ITD manages budget versus actual expenditures through the centralized PeopleSoft accounting system. Operating as an internal service fund, ITD sets its rates to cover the cost of providing services. ITD's rate setting process and annual report include comparisons to ensure that the rates are competitive with similar services offered by other states and private sector providers.

ITD monitors actual expenditures to billings through the PeopleSoft accounting system cost centers with the goal of matching billings to expenditures within each cost center. Rates are adjusted accordingly to keep costs centers within allowable reserves set forth by Circular A-87 issued by the federal Office of Management and Budget.

ITD performs an annual physical inventory of fixed assets within the department to ensure that there is adequate physical control over the acquisition and deployment of computing and network hardware.

In accordance with NDCC 54-59, ITD develops policies, standards, and guidelines for technology based on information from state agencies 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. The EA 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).

Human Resource Control

ITD's employees are its most valuable asset and ITD has formal hiring and management practices to ensure that employees are qualified for their job responsibilities.

ITD uses the ND Human Resource Management Services job classifications for all positions. The job classifications 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.

Hiring policies include performing a criminal background check on all employees. 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 ND Bureau of Criminal Investigations is contracted to perform this service for ITD.

Per NDCC 54-59-16 ITD routinely processes confidential information and its employees are subject to the same restrictions and penalties regarding disseminations of confidential information as the entity that owns the information. 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 several other policies relevant to maintaining a strong control environment within ITD.

Training of ITD personnel is accomplished through supervised on-the-job training, outside seminars and in-house classes. Organizational policies and procedures are contained in ITD's Policy Manual which is available on ITD's intranet and covered as part of employee orientation. ITD follows the NDCC and policies developed by OMB regarding annual leave accrual and cut-off dates for leave balances above 240 hours.

Formal performance appraisals are conducted on an annual basis. Completed appraisals are reviewed by senior management and become a permanent part of the employee's personnel file.

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

Monitoring

ITD management and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, each division of ITD has implemented performance measures that measure the results of various processes involved in running the data center and provided the associated services to customers. Key performance indicators are reviewed daily, weekly or monthly by appropriate levels of management, and action is taken as necessary.

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.

Per NDCC 54-59-07, the Statewide Information Technology Advisory Committee (SITAC) advises ITD regarding statewide IT planning, providing e-government services for citizens and businesses 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 provide suggestions for improvements. Survey areas include the service desk, software development, network service, E-mail services, telephone services, application hosting, records management, IT planning and oversight services, and an overall ITD rating. Results are published in ITD's strategic plan and on ITD's website.

Communication

ITD has implemented various methods of communication to ensure that all employees understand their individual roles and responsibilities. These methods include orientation and training programs for newly hired employees, an intranet site that summarizes significant events and changes occurring during the month, and the use of electronic mail messages to communicate time-sensitive messages and information. As noted earlier, managers also hold periodic staff meetings as appropriate. Every employee has the responsibility to communicate significant issues and exceptions to an appropriate higher level of authority within the organization in a timely manner. Employees participate in a formal survey every two years to identify any organizational performance issues and monitor key trends in employee satisfaction.

The organization also has implemented various methods of communication to ensure that user organizations understand the role and responsibilities and to ensure that significant events are communicated to users in a timely manner. These methods include publishing a quarterly agency newsletter titled "Information Link", conducting quarterly IT Directional meetings to

inform entities on current initiatives and issues, and meeting with key customers on a recurring basis to gather information about current and future projects. In addition, customers may subscribe to various e-mail notification systems regarding security and planned system outages to ensure they are current on issues that may affect their agencies.

ITD also publishes an annual report which includes: major accomplishments; future initiatives; ITD's performance measures and ITD's service rates which are compared with costs charged by similar organizations. ITD distributes the report to the Legislative Information Technology Committee, Legislative Audit and Fiscal Review Committee and the Statewide Information Technology Advisory Committee. The report is also available at ITD's website under "Publications".

Control Objectives and Related Controls

ITD's control objectives are listed below but the related controls are included in "Information Provided by the State Auditor's Office". This was done to eliminate the redundancy that would result from listing the controls in this section and repeating them. Although the controls are included in "Information Provided by the State Auditor's Office", they are, nevertheless, an integral part of ITD's description of controls.

Systems Development and Maintenance Control Objective 1: Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented, and documented.

Physical and Logical Access Control Objective 1: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Physical and Logical Access Control Objective 2: Controls provide reasonable assurance that logical access to system resources is reasonable and restricted to properly authorized individuals.

Computer Operations Control Objective 1: Controls provide reasonable assurance that the data center has adequate environmental controls in place.

Computer Operations Control Objective 2: Controls provide reasonable assurance that the data center has capacity monitoring and performance controls in place.

Incident Management Control Objective 1: Controls provide reasonable assurance that incidents are recorded and managed to ensure timely resolution.

Contingency Planning Control Objective 1: Controls provide reasonable assurance adequate procedures have been implemented to respond to disaster recovery scenarios.

<p>Note to Readers: The introductory paragraph to this section has been included to clearly indicate to readers that the controls are an integral part of the organization's description even though they have been presented in the service auditor's section to reduce redundancy in the report.</p>

User Control Considerations

ITD's applications and processing procedures were designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve certain control objectives included in this report. This section describes additional controls that should be in operation at user organizations to complement the controls at ITD. User auditors should consider whether the following controls have been placed in operation at user organizations.

Agency General Controls

- Controls to provide reasonable assurance that changes to processing options (parameters) are appropriately authorized, approved, and implemented
- Controls to provide reasonable assurance that transactions are appropriately authorized, complete, and accurate
- Controls to provide reasonable assurance that erroneous input data are corrected and resubmitted
- Controls to provide reasonable assurance that output reports are reviewed by appropriate individuals for completeness and accuracy
- Controls to provide reasonable assurance that output received from the organization is routinely reconciled to relevant user organization control totals

Agency Access Controls

- All data and systems in the custody of ITD have a defined owner. The defined owner is the agency responsible for the business use of the data. There is one and only one owner for each data and the owning agency appoints an agency security officer who is responsible for controlling access rights.
- ITD utilizes an on-line Work Management System where authorized users can request additions, 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 enforces 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.

The list of user-organization control considerations presented previously does not represent a comprehensive set of all the controls that may be employed by user organizations. Other controls may be required at user organizations.

INFORMATION PROVIDED BY THE STATE AUDITOR'S OFFICE

Systems Development and Maintenance Controls

Control objective 1: Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved, properly implemented, and documented.

Description of controls:

ITD utilizes a formal System Development Life Cycle (SDLC) methodology to develop and maintain applications for its customers. This methodology includes peer reviews throughout the process, based on the size and complexity of the request. These reviews are during the analysis, design and development phases and are meant to assist the developer in giving the customers a better designed solution that follows ITD standards and best practices.

ITD has a formal, Work Management System (WMS), process for requesting development work from the Software Development Division. Each user organization designates the individuals who are authorized to request program changes for their agency utilizing WMS. ITD manages changes to existing application software by documenting, prioritizing, and tracking system change requests from users. ITD monitors the change process for improvements in acknowledgment time, response time, response effectiveness and user satisfaction.

After a WMS request has been received it is reviewed to develop an estimate of the number of hours that will be required to make and implement the program change or develop the new application/system.

Once a change has been coded in a test environment, the analyst will complete initial tests and will submit a request for completion to the customer through the WMS. The customer is then responsible for testing and either accepting the deliverable via a sign-off, or documenting any issues they have found with the delivered application. The process then starts over with changes, testing, releases to customers and acceptance process until the customer accepts the final product.

Once the customer has accepted the work, a request is submitted to the ITD Computer Services division for a transfer to production.

ITD has several version control tools for maintaining the source code depending on the technology for the application. All developers have read access to the production source code. Each team within ITD is responsible for an agency or group of agencies. Individuals on the team are granted authority to access for update purposes the production source code only for the applications they maintain.

Production source code is copied to a test environment where the actual coding changes are made. The developer will unit and system test within a test environment and then send on to the agency for acceptance testing. Once the acceptance testing is completed and the user is satisfied with the results, the developer will send a project signoff request through WMS to the

customer. When the signoff is approved by the agency, this authorizes the developer to initiate the process to transfer the changes to production.

Production source code updates are completed by the developer. Object transfer requests are initiated through an automated process with additional transfer steps that are vary based on the development language for that application.

Documentation on source code changes (object name, version tool, level numbers, date of change) is recorded in WMS and updated by the developer. Any other necessary documentation is also updated by the developer and distributed to the appropriate parties.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's System Development Life Cycle process.

ITD has a formal System Development Life Cycle methodology in place that documents the steps they must follow to complete a software development project.

Conclusion

ITD assures that new applications and changes to existing applications are authorized, tested, approved, properly implemented, and documented.

Logical and Physical Access Controls

Control objective 1: Controls provide reasonable assurance that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Description of controls:

ITD coordinates with the Highway Patrol to provide physical security of the capitol complex and granting physical access to the entrance doors to ITD facilities.

ITD has locked facilities and requires all employees, contractors and visitors to wear identification badges while on the ITD premises.

ITD has camera systems in place to monitor physical access to the data center.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed the physical security procedures and policies at ITD.

We tested authorized access to key doors.

ITD has the necessary policies and procedures in place to control physical security.
--

Highway patrol manages the system that controls access to ITD's doors.
--

Door access was properly restricted to individuals needing access to the key door.
--

Conclusion

ITD assures that physical access to computer equipment, storage media, and program documentation is restricted to properly authorized individuals.

Control objective 2: Controls provide reasonable assurance that logical access to system resources is reasonable and restricted to properly authorized individuals.

Description of controls:

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

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 logout
- Unauthorized attempts to access system resources
- Resource access privileges by user id
- History of passwords and limits on password reuse
- Password complexity and change standards, as defined by the Enterprise Architecture Security Domain Team

ITD's maintains RACF security software that controls access to agency-owned datasets, library files, source code, etc. ITD also administers internal security tools for general level access auditing within SQL-server and Oracle databases.

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. The Active Directory login credentials are encrypted during transmission.

ITD, in conjunction with 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'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 to "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.

ITD has implemented Intrusion Detection Systems and performs regular vulnerability assessments on its computing and network infrastructure to proactively identify systems with high risk profiles.

ITD deploys SSL encryption where appropriate.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's security policies and procedures.

We reviewed ITD's Work Management System (WMS) for security requests. To properly notify ITD of security requests through WMS, agencies should have policies and procedures for adding, changing, and removing their employee's access.

We reviewed ITD's incident response procedures and intrusion detection system.

ITD has security policies and procedures, but lacks a formal security plan.

ITD has a system that allows agencies to communicated changes to user accounts to them.

Security violations are sent to agency security officers for review daily.

Yearly reports showing authorized user accounts are sent to agencies to review and certify.

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 plans to develop a formal security plan. ITD does have dedicated security staff that focus on enterprise security issues and procedures, however we do agree that there is value in formalizing existing processes and standards into an overall plan.

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 plans to work with security organizations in other states to determine best practices in this area as we formalize our risk assessment processes.

Conclusion

ITD assures that logical access to system resources is reasonable and restricted to properly authorized individuals. The finding and recommendation noted are meant to improve the efficiency and effectiveness of security offered by ITD and does not, in our view; represent significant issues that would affect the overall assessment of security at ITD.

Computer Operations

Control objective 1: Controls provide reasonable assurance that the data center has adequate environmental controls in place.

Description of Controls:

ITD's Data Center 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. The 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 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.

Subsequent Event Disclosure – Jan. 18, 2011 Power Failure

At 10:43 AM on Tuesday, January 18, 2011, a failure occurred in the electrical transformer feeding power to the Judicial Wing of the State Capitol. The transformer is located between the electrical generator and the Judicial Wing and prevented the generator from providing backup power to the Bismarck Data Center.

ITD implemented its Disaster Recovery Teams and relocated its Management Operations Center as outlined in our Continuum of Operations Plan. ITD began to provision the equipment at the Mandan Data Center to assume the role of the primary data center. When electrical engineers indicated that power would be restored to the Bismarck Data Center at approximately same time the Mandan Data Center would be able to assume the role of the primary data center ITD decided to keep the Bismarck Data Center configured as the primary site to allow all services to come on-line rather than just the systems that had been architected for business continuity.

OMB and ITD are working with electrical and data center consultants to implement additional power redundancy to the Bismarck Data Center and improve the recovery time objective for the Mandan Data Center to assume the role of the primary data center for any future disaster events.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's environmental protections in the various key rooms.

We toured the rooms to ensure the protections were in place and working.

The necessary protections from fire, water, humidity, and temperature are in place. Facilities Management monitors, tests, and maintains the environmental sensors and alarms.

The Mandan data center has smoke detectors, raised flooring, air conditioning and temperature and humidity sensors (monitored by ITD). There are no water sensors or fire suppression at this facility.

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

Conclusion

ITD assures that the data center has adequate environmental controls in place.

Control objective 2: Controls provide reasonable assurance that the data center has capacity monitoring and performance controls in place.

Description of Controls:

ITD schedules mainframe / mid-tier 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. These planned downtimes allow for proactive system maintenance to be performed.

ITD monitors computer and network operations performance based on assessments of individual systems and available performance capacity system software. Performance management reports include 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. In addition, 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 minimize data loss due to hard drive failures.

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

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

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 of its Intel computing platform (hardware, O/S software, applications software, facilities and data files) through HP's Systems Insight Manager software configuration tools and Altiris software.

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

ITD Computer Systems Division 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.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's policies and procedures for monitoring capacity on existing systems.

We reviewed ITD's policies and procedures for ensuring availability of systems.

We reviewed ITD's performance and capacity monitoring on three systems.

ITD monitors its systems to ensure adequate capacity exists.

ITD ensures that its systems are available and schedules downtime on them with the affected agencies.

Conclusion

ITD assures that the data center has capacity monitoring and performance controls in place.

Incident Management Controls

Control objective 1: Controls provide reasonable assurance that incidents are recorded and managed to ensure timely resolution

Description of Controls:

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

ITD's Help Desk receives requests via telephone, the Help Desk web site and email. They log and track all requests using FrontRange Solutions – ITSM System. ITD has implemented ITSM 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

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

ITD has a formal incident response policy and team that is used when responding to security related incidents.

Tests of Operating Effectiveness and the Results of Those Tests

We reviewed ITD's help desk policies and procedures.

We reviewed the latest performance measures for the Help Desk.

ITD has an automated solution for documenting and tracking incidents.

ITD monitors the timeliness and satisfaction of resolutions.

Conclusion

ITD assures that incidents are recorded and managed to ensure timely resolution.

Contingency Planning Controls

Control objective 1: Controls provide reasonable assurance adequate procedures have been implemented to respond to disaster recovery scenarios.

Description of Controls:

ITD maintains a disaster recovery hot site in Mandan, ND. The hot site facility provides replication of critical data and selected application servers. It houses full daily backup tapes for file recovery or complete system restore, if needed.

ITD performs a regular testing its Disaster Recovery Plan at the hot site facility. Tests include restoring the IBM mainframe, AS/400, and other selected processing platforms. 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 is a fire extinguisher located inside the off-site vault. ITD updates the vault combination upon employee turnover, or annually at a minimum.

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'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 examined ITD's continuity planning procedures.

We examined ITD's disaster recovery plan.

We inspected the Mandan Data Center and backup site to ensure they contained the necessary information.

We reviewed documentation of ITD's disaster recovery testing.

ITD has a Disaster Recovery Plan in coordination with the states Continuum of Government plan.

ITD has a secondary data center that can be used in the event of a disaster.

ITD performs a series of small disaster recovery on their plan.

Conclusion

ITD assures adequate procedures have been implemented to respond to disaster recovery scenarios.