ITD North Dakota
Information Technology Department

SOC3-Service Organization Control Report

ITD

For the Period of July 1st 2015 through June 30th 2016

Uriah Burchinal
Author
Sean Wiese
CISO

4201 Normandy Street
Bismarck, ND 58503
(701) 328-3190

Table of Contents

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

Independent Auditor's Report

The Honorable Jack Dalrymple, Governor
Members of the North Dakota Legislative Assembly
Mike Ressler, Chief Information Officer

Scope

We have examined the Information Technology Department's (ITD) Description of System and Controls-2016 for the period July 1, 2015 to June 30, 2016 and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of Information Technology Department's controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

The Information Technology Department uses Multi-State Information Sharing & Analysis Center (MS-ISAC) for intrusion detection services. Our examination did not extend to controls of the computer processing service organization.

Service Organization's Responsibilities

On page 1 of the description, the Information Technology Department has provided the attached about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives state in the description. The Information Technology Department is responsible preparing the description and for its assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2015 to June 30, 2016.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described at page 5. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions in providing networking services, electronic mail, file and print server administration, database administration, storage, application server and hosting services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in the Information Technology Department's assertion on page 5.

a) The description fairly presents the system that was designed and implemented throughout the period July 1, 2015 to June 30, 2016.

b) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2015 to June 30, 2016 and user entities applied the complementary user entity controls contemplated in the design of XYZ Service Organization's controls throughout the period July 1, 2015 to June 30, 2016.

c) the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2015 to June 30, 2016.

Restricted Use

This report including the description of tests of controls and results thereof are intended solely for the information and use of the Information Technology Department; user entities of the Information Technology Department during some or all of the period July 1, 2015 to June 30, 2016, and the independent auditors of such user entities, who have sufficient knowledge and understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Bob Peterson

Robert R. Peterson
State Auditor

Edwin J. Nagel, Jr.

Edwin J. Nagel, Jr., CPA
Director

Bismarck, North Dakota

November 17, 2016

ITD Management Assertion

Assertion by Management regarding State of North Dakota Information Technology Department service organization operations throughout the period July 1, 2015 to June 30, 2016

We have prepared the enclosed description of ITD's operation as a service organization. This service organization system description provides an explanation of the controls relevant to Security, Availability, Processing Integrity, and Confidentiality during some or all of the period July 1, 2015 to June 30, 2016.

We confirm, to the best of our knowledge and belief, that the description fairly presents ITD's service organization system made available to state entities as stipulated under North Dakota Century Code (NDCC) 54-59. The criteria we used in making this assertion were that the description presents our control environment, risk assessment process, information and communication systems (including related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of state entity users of ITD systems.

Additionally, this system description does not omit or distort information relevant to the scope of ITD's operation as a service organization and it is prepared to meet the common needs of a broad range of state entity users of the system and the independent auditors of those entities.

We confirm, that to the best of our knowledge and belief, that the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period to achieve those control objectives.

Description of Service Organization's System

Scope and Purpose

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 (CIO) who reports directly to the Governor. This document describes the control structure of ITD as it pertains to hosted services. The system is defined as the network, hardware, operating systems and middleware used by ITD in order to provide services to state agencies, including institutions under the control of the State Board of Higher Education, counties, cities, and school districts hereafter referred to as user organizations. Professional services work done by ITD on the behalf of an agency such as application development and desktop support are not a hosted service and therefore excluded.

Overview of Services Provided

ITD is responsible for providing and maintaining the underlying IT infrastructure that provides the base or foundation for the state's information technology systems. Infrastructure includes (1) hosting computer systems or hosting middleware; and (2) network services that accommodate the data, voice, video, and multimedia traffic over a statewide backbone to support the missions of government and education.

1. **Hosting**

Databases

ITD operates dedicated equipment necessary to host user organization database applications.

Datacenter Space Rental

Datacenter Space Rental provides a managed facility for customers to locate servers and related computer equipment over which they retain ownership and operational authority.

Despite the remarkable transformation of the state IT enterprise over the past decade, states can be even more responsive and more capable in delivering services and protecting the states' data systems and information. That capacity rests critically on the task of reengineering business processes and eliminating redundancies whenever possible. State CIOs have seized on the potential for galvanizing the state IT enterprise to produce better results and reduce costs by engaging in consolidation of state data centers for optimizing the physical infrastructure and to streamline business functions

Disk Storage & Backup

ITD offers several levels of storage services, including automated backup services.

Tiered Solutions

- Basic Storage
  Designed for non-critical data that does not require high performance or high availability.
- File Share Storage
  Designed for critical documents, images, other non-transactional data that requires high performance and high availability.
- Premium Storage
  Designed for critical database and transactional data that requires high performance and high availability.

Backup/Recovery

Tapeless backup (disk-based) and tape storage is provided for all disk storage services.

Replication

Replication creates a real-time copy of data in both the primary and secondary datacenters and significantly improves recovery time in the event of a disaster.

File & Print

File and Print services allow people to store, secure, share, and print files over the network.

A file server's primary purpose is to provide a location for shared file access, i.e. shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by workstations attached to the network. It is designed primarily to enable the rapid storage and retrieval of data and share this information with others.

A print server's primary purpose is to provide print job management to shared printers.

Hosting Platforms

ITD provides hosting services for a number of hardware platforms. ITD’s hardware hosting catalog includes the following:

Intel Servers

ITD hosts a variety of application servers in a stand-alone, clustered and virtualized environment. All of these operate in our secure and environmentally controlled data center facility.

ITD uses a blade infrastructure that helps to lower cooling and electrical costs and reduces space requirements. We support both Linux and Windows operating systems with over 94% of servers running in a virtualized system.

Midrange (IBM iSeries) AS/400

ITD provides hosting services (including computer processing and electronic storage of data) for the IBM iSeries platform. The IBM iSeries, formerly known as the AS/400, is a mid-range server designed for small businesses and departments in large enterprises.

IBM Enterprise Server (Mainframe)

A mainframe is a high-performance computer used for large-scale computing purposes that require greater availability and security than a smaller-scale machine can offer.

The mainframe is the classic centralized computing system. Even though the mainframe platform is not strategic to new application design, it remains a fully-supported modern platform for legacy applications.

Web Server & Middleware Platforms

ITD has a number of hosted solutions for both web sites and web applications. ITD’s web service hosting catalog includes the following:

Websphere

IBM's Web Application server. ITD provides the equipment necessary to host agencies websphere applications. The cost is tiered based on the size and complexity of the application

.NET

Microsoft's web application server; runs on the Windows Server platform.

IIS (Internet Information Services)

Microsoft's older web server; runs on the Windows Server platform.

Apache

An open source alternative for web servers; uses ITD's Linux infrastructure

2. Network Services

Local Area Network

ITD provides managed Local Area Network (LAN) service for a building or campus environment enabling data communication among local computing and printing resources within a user organization.

This service is typically only available to customers within the state government user space. Solutions may vary depending on location, however they typically include service to the endpoint "jack in the wall" with connection capacities ranging from 10mb, 100mb, and 1g.

Wide Area Network

The statewide WAN provides gateway services to the public internet and functions as a private fault-tolerant network allowing for interconnectivity within STAGEnet. ITD manages the statewide WAN for all user organizations. Connection to the statewide WAN can be achieved by a variety of methods to meet the technical and financial requirements of a facility.

Major Metro Area Network presently exist in Bismarck and Fargo. These solutions provide for a resilient fault tolerant core network that provides dual redundant fiber paths to key locations. The MAN provided redundant connections to the WAN allow for sites to connect to the network with single or dual fiber solutions.

Fiber connections are available in most locations. Fees vary depending on location and construction costs may be required. The fiber connections can be connected to a variety of aggregation points including the WAN, MAN, or other aggregation points in a community.

Ethernet Transport Service (ETS) solutions exist in most locations across the state. This service starts and 5Mb and can scale to 1g and beyond.

Broadband solutions exist in many communities across the state. The solutions can be DSL or cable solutions with capabilities that vary in each community. Broadband solutions are connected to aggregation points on the statewide WAN and secured via a site-to-site VPN.

Custom Solutions are available in a variety of options to any location.

Wireless Network

ITD provides a managed and monitored 802.11abgn wireless network solution that can be installed in user organization locations.

This service is customized depending on customer requirements, and it can include public access and/or authenticated secured connections. Wireless service is typically deployed with both public access and secure authenticated access to STAGEnet.

STAGEnet-Guest; unencrypted access to the Internet using a real external IP address. Service is available authentication to any customer with a compatible wireless device.

STAGEnet-Member; authenticated and encrypted access to the internal network without the use of a Virtual Private Network (VPN).

Relevant Aspects of the Overall Control Environment

1. Control Environment

ITD's control environment is developed around the ITD Cybersecurity Framework. This framework is based on the NIST Framework Core and addresses protecting systems by using the functions to identify, protect, detect, respond, and recover. Following the ITD Cybersecurity framework ITD uses the NIST 800-53 r4 control set in order to achieve the framework outcomes as well as adhering to regulatory mandates.

2. **Control Activities**

   ITD's organizational structure provides an overall base for planning, directing and controlling operations and is the responsibility of executive management. The CISO is ultimately responsible for the security controls with the assistance of the executive management team.

3. **Risk Assessment**

   As part of ITD's Risk Management Plan a formal process has been implemented to assess the threats and vulnerabilities that give rise to inherent risk of the overall organization. Risks Identified by assessments are reviewed and addressed in order to close any control gaps and reach a residual risk profile that is acceptable.

4. **Monitoring**

   Monitoring of controls occurs through ongoing audits and periodically required federal responses to identified weakness. ITD also performs annual security assessments that includes a controls gap analysis.

5. **Information and Communications**

   The hosted services provided by ITD utilizes a network of hardware, systems software, and telecommunications systems. Communications between user organizations and these data centers occur over a statewide communications network referred to as STAGEnet.

   Corporate wide controls are communicated through the ITD Cybersecurity Framework and ITD policies that accompany them as well as statewide standards developed by the Enterprise Architecture Team.

Control Objectives and Description of controls

The following is a description of the internal controls that are generally considered to be part of ITD's control environment. The overall control structure of ITD consists of specific control activities that can be related to ten (10) major areas. These areas are defined by the Trust Services Criteria.

- Organization and management
  Criteria is relevant to how the organization is structured and the processes the organization has implemented to manage and support people within its operating units

- Communications
  How the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.

- Risk Management and design and implementation of controls
  How the organization identifies potential risks that would affect the entity's ability to achieve its objectives, analyzes those risks, and develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and conducts ongoing monitoring of risks and the risk management process.

- Monitoring of controls
  Criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.

- Logical and physical access controls

Defines how ITD restricts logical and physical access to systems, provides and removes that access, and prevents unauthorized access.

- System operations
  Addresses how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations.

- Change management
  The criteria relevant to how the organization identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principle(s) addressed in the engagement

- Confidentiality
  Confidentiality is ensuring that information is accessible only to those authorized to have access, regardless of where the information is stored or how it is accessed.

- Availability
  Data Integrity is defined as safeguarding the accuracy and completeness of information and processing methods from intentional, unauthorized, or accidental changes.

- Integrity
  Availability is ensuring that authorized users have access to information and associated assets when required.

The primary objective of the control structure is the establishment of an appropriately controlled environment to develop and implement policies and procedures to achieve internal control objectives that are aligned with the ITD Cybersecurity Framework.

1. Organization and Management

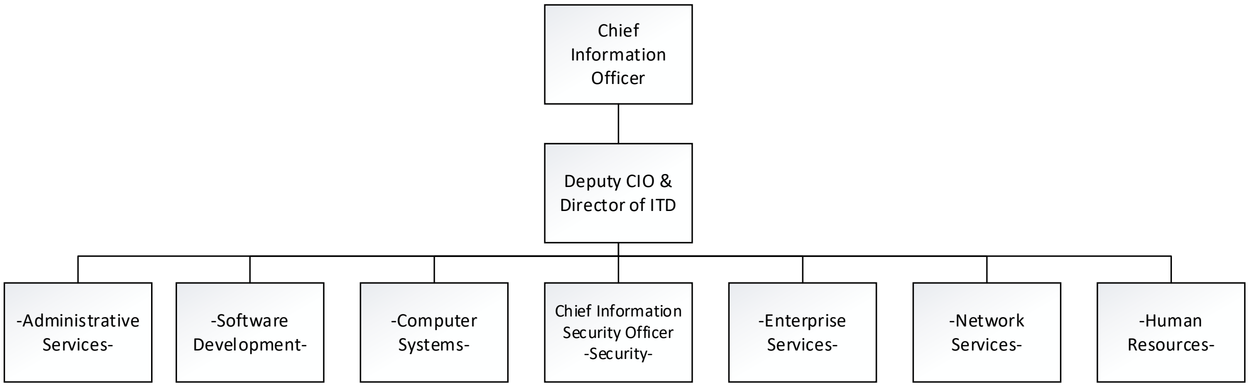
ITD has adopted the following six guiding principles that provide the foundation for the organization and set standards for how employees and managers are expected to act and interact:

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

The ITD exists for the purpose of leading user organizations in discovering, assessing, and implementing information technologies. ITD is committed to better understanding user organization needs and in assisting in the implementation of the proper technology solution to accomplish those needs. ITD is organized to provide a broad range of technologies including mainframe and desktop computing, local and wide area networks, voice and data technologies, web, client server and mainframe software development, video conferencing, and emerging technologies. This is accomplished by investing in the development of highly skilled employees along with contracting outside vendors who maintain a level of expertise that is not available in-house or is limited due to the demands for a particular service.

ITD's mission is to provide leadership and knowledge to assist our customers in achieving their mission through the innovative use of information technology.

ITD has defined a hierarchical organizational structure with each division responsible for the security, availability, processing integrity, confidentiality, etc. of their respective areas. ITD has also implemented a Chief Information Security Officer, which has the authority over the Security Division and subsequent security program, as well as the responsibility to collaborate across organizational lines to ensure security, integrity, etc. of the State's computing resources.


Chief Information Officer
Deputy CIO & Director of ITD
-Administrative Services-
-Software Development-
-Computer Systems-
Chief Information Security Officer -Security-
-Enterprise Services-
-Network Services-
-Human Resources-

The seven divisions outlined above include over 300 employees providing the following services to ITD's customers:

Administrative Services - Provide accounting functions, assist customers with billing and oversee strategic initiatives related to budgeting and records management.

Software Development – Develop and maintain computerized applications and provide related consulting services. Responsibilities include design, development, and support of customized software applications that operate on a variety of computer platforms and database management systems. Staff are 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.

Computer Systems - Provide technical computing infrastructure and the expert skills required to host the state's applications, including clustered servers, redundant storage, multi-path networks, environmentally controlled data centers with generator backup and uninterpretable power supply systems. Provide round-the-clock job processing and routine system procedures required during the non-business hours.

Enterprise Services – Coordinate ITD's people, process, and technology in a way that promotes customer-centric services. Foster customer relations and align ITD's services with customer expectations. The Service Desk is the heart of this division. This division also contains enterprise program administrators that assist user organizations with setting direction and maximizing the value of technology investments.

Network Services – Oversee the statewide network providing broadband connectivity, internet access, video conferencing and other networking services to user organizations, local government, higher education, and K-12 schools. Ensure the reliability and security of statewide network from the threats of viruses, worms, and hackers. The division is on-call 24/7 to ensure information flows freely to the right people, at the right place, at the right time.

Human Resources - Provide a variety of services to ITD, including the following: recruitment, selection, and retention of highly qualified employees; strategic planning assistance; policy implementation; job classifications maintenance; employee/manager relations; benefits; compensation; legal compliance; training and development; and risk management & workplace safety.

Security - Is tasked with designing, developing, and monitoring controls. The implementation, operation, and maintenance of controls is the responsibility of the respective divisions that oversee the systems and processes the controls apply to. Approval of system controls is done is performed by the executive management team and is coordinated by the CISO.

ITD has established workforce conduct standards, background screening procedures, and enforcement measures by way of information policy and procedures.

The Cybersecurity Framework includes a Statement of Management Commitment and provides an overview of the roles and responsibilities for various officials and organizational offices involved in cybersecurity.

2. Communications

The design and the operation of systems and its boundaries is documented. Detailed architectural documents are maintained in an internal Wiki. Access to the Wiki is limited to ITD Architects and Executive management. High level design documents provided to internal and external users of the system are available and provided as needed. Ongoing operational documentation is maintained by system administrators responsible for system operation.

Security commitments are communicated to internal users through policy and annual awareness training. Service level agreements, business level agreements and contracts all communicate levels of responsibility for all parties whose role affect system operations. Information needed for a user to carry out their responsibilities are provided.

Failures, incidents, concerns, and other complaints are submitted through a call or email to the ITD service desk. These items have a ticket opened and are documented and resolved within timeframes designated in the service level agreement

System changes are communicated through the change management process.

ITD provides services to a variety of customers and ensures open and timely communicate through the following methods:

- An intranet site that summarizes significant IT events and changes occurring during the month.
- E-Mail messages to communicate time-sensitive messages and information.
- Quarterly agency newsletter titled “Information Link”.
- Quarterly IT Directional meetings to inform entities on current initiatives and issues.
- Meetings with key customers on a recurring basis to gather information about current and future projects.

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".

Procedures have been implemented for sharing information with third-parties, which is accomplished through Information Exchange Agreements (IEA).

3. Risk Management and Design and Implementation of Controls

ITD’s CISO along with the executive 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 CIO, Deputy CIO, CISO, and Division Directors.

ITD has placed into operation a risk assessment process to identify and manage risks that could affect the ability to provide reliable transaction processing for user organizations. This process requires management to identify significant risks in their areas of responsibility and to implement appropriate measures to address those risks. The agenda for each quarterly management meeting includes a discussion of these matters. This process has identified risks resulting from the nature of the services ITD provides, and management has implemented various measures to manage those risks.

ITD identifies potential threats through a yearly security assessment of the control structure through the use of the Cyber Security Evaluation Tool provided by the Department of Homeland Security. The security assessment is run against NIST 800-53 moderate controls to identify potential risk. ITD also commissions a penetration test every two (2) years. The outcome of the security evaluation and penetration test is analyzed and mitigation and remediation strategies are put in place. Policies, standards and procedures, are evaluated based on the risk mitigation plan to implement achieve the risk mitigation strategy.

Changes that could affect ta system's internal control are evaluated by the presence of a security division representative on the Change Advisory Board. Mitigation strategies are reassessed if required due to a change.

4. Monitoring of Controls

The effectiveness of controls are evaluated against requirements on an ongoing basis. The controls in place are audited against federally on average every three years. A Service Organization Controls audit is performed by the State Auditor's Office every two (2) Years to assess the controls in place. Federally required audits for specific agencies include ITD controls for hosted systems. These audits occur approximately every three years. ITD is required along with the agency to submit quarterly responses in the form of Corrective Action Plans and POA&Ms.

5. Logical and Physical Access Controls

ITD has implemented Active Directory as the mechanism for logical access to provide an identification, authentication and authorization mechanism. Active Directory is used to restrict access to both the system and components thereby preventing unauthorized access. All users are both identified and authenticated when accessing the system.

All user organizations networks using Active Directory coordinate their installation and maintenance activities with ITD to ensure that all networked Active Directory computers are members of the State forest, NDGOV. Organizational Units (OU) are used to create grouping of computers, users, and groups to provide for the delegation of administrative control of the agency network.

The Enterprise and Domain Administrator role/responsibilities reside with ITD. ITD will only grant access to information based upon authorization requests from Agency IT Coordinators.

The OU administrators can limit the rights of the Enterprise and Domain Administrators to the domain controllers within the active directory forest. However, the Enterprise Administrator does retain the right to remove these restrictions. This is a fail-safe feature to allow the Enterprise Administrator the ability to repair any damage to the Active Directory. While this is a necessary enterprise feature and requires modification to the OU security, all such access by the Enterprise Administrator is monitored and logged.

New users are registered and authorized based on the role they will be filling with ITD. Human Resource process ensure proper authorization of users as well as the removal of such authorizations when the users is terminated or transferred.

Access to all system components and functions are authorized based on the roles and responsibilities of the system users. Physical access to sites is restricted to only personnel that needs access to the site in order to fulfill job duties and customer commitments. Transmission, movement and removal of information is protected and restricted as required by both requirements and policy.

All servers and workstations administered by ITD require users to logon prior to being granted access to system resources. To ensure security and confidentiality, all Active Directory login credentials are encrypted during transmission. Local guest and anonymous accounts have been deactivated or deleted. All workstations located in an area of public access are configured to provide only the services needed. All workstations have automatic screen locking active with a maximum of a 15-minute activation time. Servers and workstations are required to be either manually logged off or locked prior to leaving them unattended.

Unique user IDs and passwords are assigned to each user, and initial passwords and passwords reset by administrators are one-time passwords that are required to be changed at next use. A web application has been created to allow authorized individuals to unlock Active Directory accounts. ITD has a centrally managed password management system in an encrypted database.

For guest and system supplied user IDs that cannot be removed or disabled, the default password is changed. For network infrastructure devices, all default authentication credentials are required to be changed during setup.

ITD issues general credentials for ITD staff that allows them access to basic e-mail, file, and print services. These credentials are not granted Administrator level access. Staff that require Administrator access are issued a separate set of credentials to administer IT systems. The Administrator access granted is the least privilege necessary to perform the job function effectively

Wherever possible, individual credentials are used to administer ITD resources. When shared credentials are necessary they are changed every 60 days and immediately when a staff member with security privileges terminates their employment with ITD. Additionally, ITD automatically disables accounts after 60 days of inactivity.

Unauthorized malicious software is prevented and detected through both network protections and end point protections. ITD, in conjunction with the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address the prevention and detection of computer viruses and the installation of virus prevention software and critical updates. ITD uses virus and spyware detection programs on all workstations and servers. In addition ITD deploys additional appliances at key locations on the network to monitor virus activity.
Anti-Malware software has been installed and active on all devices that can effectively run an anti-malware or anti-virus client. Auto-distribution of current anti-virus signature files has been configured. All incoming files, including email, are scanned in real-time for malware. In addition, all files are scanned for malware on a weekly basis. Files containing malware which cannot be cleaned are deleted.

ITD resides within a locked facility and utilizes identification badges to grant access to restricted areas and to ensure that only authorized personnel are in restricted areas. ITD employees and contractors are required to wear their badges while on ITD premises. Contractors who have had security background checks are allowed unescorted access to ITD premises specific to the project they are working on.

Visitors to ITD datacenters are required to sign-in at one of ITD's reception areas and wear Visitor badges. Visitors are not permitted unescorted access at ITD datacenters. Visitor logs serve as audit records for physical visit reconstruction.

ITD maintains a video surveillance system for critical ITD entry points. The video logs are maintained for approximately three weeks and are used to investigate security or personnel incidents. ITD receives usage reports from the Highway Patrol who manages the door access system. These reports are reviewed by security and data center staff for inappropriate access attempts.

Physical security to facilities housing ITD equipment and personnel is also controlled via multiple physical barriers. Media-storage areas (key-locked cabinets, tape vaults, etc.) are doubly secured via badge-reader and traditional key-lock countermeasures.

6. System Operations

Vulnerability scans are run on a regular basis on base infrastructure components. Specific vulnerability scans are run at user organization's request at a frequency determined ate their request. Vulnerabilities are evaluated and sent to the responsible administrators for resolution.

Networking equipment monitors for signatures including know vulnerabilities. A managed security appliance is provided and monitored by MS-ISAC for alerting and reporting of threats in real time.

A security incidents plan has been developed as well as policy and procedures for the handling of security incidents. This includes the defining of security incidents, handling evidence, investigative practices, roles, responsibilities and lines of communication. This plan includes communication requirements set forth by the user organization.

Incident Response is coordinated by the ITD Security Division and is responsible for ensuring that ITD responds to security incidents in a timely and effective manner. An individual has been designated to coordinate the incident prevention/response/notification process throughout ITD. Incident response contacts are designated by each user organization. The ITD coordinator communicates incidents or vulnerabilities to user organization contacts. The user organization contact communicates any incidents or vulnerabilities to appropriate personnel.

ITD maintains a Security Information Event Management (SIEM) system to store centralized log information. This system is used to identify and prioritize potential security events for investigation.

ITD, in conjunction with the Enterprise Architecture Security Domain Team, has implemented policies and procedures to address firewall management, intrusion prevention and detection, and remote access. ITD adheres to the concept of least privilege necessary when configuring and administering the State's IT infrastructure. Accordingly, network and system administrators only enable the services or ports that are necessary for the equipment or application to perform its necessary business function. This principle includes but is not limited to the following infrastructure components: Servers, Switches, Firewalls, and Applications. Where applicable, ITD deploys Secure Socket Layer (SSL) encryption. Third party solutions such as LogMe In or GoToMyPC are expressly prohibited and, where possible, are blocked. ITD utilizes a content filtering appliance to filter access to Internet sites and materials it deems inappropriate for business use.

Firewalls have been implemented to protect the State's network and computing resources from untrusted sources. The ITD Network Firewall Group administers firewalls based upon authorized service requests passed through the Work Management System after review by the ITD Security division. ITD's policy over firewall control is to lock down all access and open only authorized ports and hosts that require access. 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. Where possible, ITD utilizes automated procedures to respond to event anomalies.

ITD utilizes the state Virtual Private Network (VPN) for all remote access connections other than those that are externally available outside the state firewall. ITD system and network administrators only use state-owned computers and state-owned mobile devices that adhere to ITD’s mobile device access standards for access to systems when using their Administrator credentials

7. Change Management

ITD evaluates and addresses requirements of systems throughout the system lifecycle. ITD works in conjunction with the user organization to ensure all requirements are in place. All system components are updated as defined by rudiments as they change. Identified deficiencies are addressed if discovered.

Changes to system components are implemented through the change management process. Changes to the system can be initiated by either ITD or at the request of the user organization. Testing is carried out on all changes as appropriate. Users and stakeholders review and approve results of testing prior to implementation. A request for the change is put in through a formal process and then reviewed by the change advisory board. Once approved all affected entities are notified of the change. Once the change is implemented another notice is sent.

Emergency maintenance may be done outside of the standard Change Windows and without 48-hour notice. Emergency changes must be logged. Divisional staff may expedite the voting process, and assume full responsibility, by changing the status to “Approved” at any time. If possible, it is helpful to use a status of “Accepted Divisionally” for a short period of time to allow internal discussion.

8. Confidentiality

User organization information is protected throughout the system lifecycle. Information is accessible only to those who need such access to perform the functions of their roles. Information is protected against unauthorized access, use or disclosure. ITD works in conjunction with the user organizations to ensure that requirements are defined and met as needed.

Access to information outside of system boundaries is not allowed unless so directed by the user organization. ITD contracts with third party organizations specifically address confidentiality. Contractor requirements set forth by the user organization are followed as designated by the user organization. Changes to confidentiality commitments and requirements are communicated to all applicable parties.

On an annual basis, ITD employees and contractors are required to sign an acknowledgement document that references North Dakota Century Code § 12.1-13-01. This document relates to the disclosure of confidential information provided to government and states, “A person is guilty of a class C felony if, in knowing violation of a statutory duty imposed on him as a public servant, he discloses any confidential information which he has acquired as a public servant. ‘Confidential information’ means information made available to the government under a governmental assurance of confidence as provided by statute.”

See the section above entitled Security Access and Management for an overview of controls related to logical and physical access, including data and resources considered confidential. Individual agencies must establish logical access control consistent with the EA Standard – ST006-04.6 –Access Control and EA Standard – ST004-04.1 – Active Directory.

The standards outlined in G002-99 – Information Technology Contract Guidelines provide specific guidelines for establishing a contract with third-party technology providers along with applicable confidentiality requirements.

Encryption is used when the electronic transmission of information involves sensitive data that passes over the public network. Sensitivity of data is determined by the government entity administering the data or the application. Where possible, ITD utilizes the following encryption methods:

- Full disk encryption on all portable devices.
- Secure Socket Layer (SSL) Encryption for all web applications that require authentication and/or process sensitive data.
- Encrypted e-mail solutions for staff and customers that require e-mail encryption.

In accordance with ST002-04.1 *Remote Access Standard*, all remote access requires encrypted communications, and all external connectivity to the internal state network utilizes a VPN. All VPN connectivity is authenticated and authorized by the enterprise authentication/authorization process. Authentication for remote access to servers is provided by the central authentication server and requires registered user ID’s. Where data encryption is used, the government entity administering the data or the application is required to have a recovery plan for encryption keys.

9. <u>Availability</u>

Capacity is evaluated and planned for to ensure availability starting with architectural of the environment. The usage of system capacity such as disk space, processor, memory, and bandwidth is monitored and maintained through various tools that report and alert based on predefined criteria. This allows the system to be managed and provide for all capacity needs in a timely manner.

Recovery of the infrastructure is planned for and documented with prioritization of services defined and reviewed. Backup and replication systems are monitored and responsible parties are alerted in the event of a failure. ITD has established formal policies and procedures that outline requirements for agencies to review their data and identify backup requirements. These standards also indicate that backup procedures must adhere to the Continuum of Government guidelines. Requirements for backup of systems is primarily covered by the Enterprise Service Level Agreement and thereafter the Hosting Service Level Agreement.

Daily off-site backups are provided for all data hosted and source-code written by ITD. Databases have full weekly backups and nightly incremental backups, while other datasets only backup items that have changed during the day. Large-scale storage of static data typically warrants an alternative custom backup configuration.

Service level objectives for backup reliability include:

- There will be less than two failed/cancelled full or incremental backups per month
- Successful backups are expected 99.00% of the time, with a minimum of 95.00%
- Successful recoveries are expected 99.00% of the time, with a minimum of 95.00

ITD’s Computer Operations Manager and support staff receive an itemized list of tapes from backup administrators. These tapes are outputted at the secondary data center from the tape library system to be transported to the offsite backup location. These tapes are gathered and transported to the offsite location. Additionally, this process identifies tapes that are already in the offsite location for return to the tape library. These tapes are gathered and transported to the secondary data center for return to the tape library.

ITD supports near real time failover. Systems are manually failed over, allowing ITD to assess the incident and make decisions based on all factors of the incident

Procedures supporting system recovery in accordance with recovery plans tested as defined and agreed upon with each induvial agency as directed by that agency.

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. The data center has a raised floor, smoke detectors, air conditioning, and security camera. Agency personnel are allowed access to the room through their key cards.

ITD maintains a disaster recovery hot site. 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. At this facility, ITD maintains a back-up of the current client server and mainframe operating systems, start-up instructions, a copy of the disaster recovery plan, and a recovery priority list of mainframe and mid-tier applications. The 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 performs 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. External agency personnel also participate in the testing process to validate recovery of their applications.

10. Integrity

ITD is responsible for maintaining the storage integrity of the information as submitted by user organizations. Information is backed up and stored as agreed upon with the user organization. These backups ensure that the information is in the same state as it was when submitted.

Backups to tape will alert on excessive CRC errors. Backup errors and issues are monitored and addressed by ITD storage administrators. Backups made to disk (virtual tape) are monitored for excessive I/O errors.

No data modifications are made by ITD staff unless directed to do so by the user organization through a support ticket. Modifications are documented and only performed by staff that is responsible for the system in questions and qualified to do so.

SQL integrity is a check performed to insure that the data written to disk maintains integrity. SQL server writes a checksum to each 8K data page. During an integrity check SQL Server reads each data page in a database and calculates the checksum to compare against the stored value. If a mismatch is found the check shows up in a weekly email to DBA’s. Most of the time a page can be repaired by using existing data using SQL commands built into the engine. As an alternative it can be repair by restoring a backup copy of the table, index, or other object affected.

SQL Backups run nightly and ITD DBA’s use a policy checker tool to verify each database has a successful backup. Databases with missing backups can be added to the backup schedule according to the customer’s needs. In addition other policy checks validate security rights, database parameter settings, or other SQL server settings deemed necessary to monitor.

ITD’s Enterprise and Hosting Service-Level Agreement (SLA) provides tailored solutions such as IBM WebSphere and its associated components, which generate security exceptions (alerts/events) in cases of abnormal server states, resource utilization, and/or transaction outcomes. Firewall logs of repeated failures and auto-blacklist actions are reported as security alerts to a Security Information and Event Management (SIEM). Additionally, service monitoring systems comprise ancillary error/exception alerting mechanisms (e.g., unsuccessful or unusually slow HTTP GET).

The tables below outline Enterprise Architecture (EA) standards that have been established related to the integrity of data handled by ITD systems.

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.

- 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.
- ITD does not own most of the information residing inside ITD's information systems. The information owner for most data is the user organization.
- 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 ITD is routinely reconciled to relevant user organization control totals

User Entity Control
User organizations are responsible for establishing security access administration policies and procedures for the allocation of user IDs, passwords and access levels which are created by client system administrators.
User organizations are responsible for maintaining the confidentiality of system user IDs and passwords.
User organizations are responsible for timely written notification to ITD of changes to authorized security officers administrators, and persons authorized to approve access requests.
User organizations are responsible for the administration and tracking of Security awareness training within their organizations.

User organizations are responsible for sending authorized requests to ITD for updating access related to a change in an employee's job function, new employment, or termination.
User organizations should establish their end users in such a way that segregation of duties is achieved.
User organizations should configure workstations to enforce a session time-out after a period of activity.
User organizations are responsible for establishing and maintaining physical security of all user offices and computer equipment.
User organizations are responsible for limiting physical access to only those individuals that require such access to perform their jobs.
User organizations are responsible for approving and testing changes and updates.
User organizations should have procedures in place to require management authorization of requests for ITD to change or customize their environment.
User organizations are responsible for individualized Disaster Recover Plans and working with ITD to ensure proper requirements and agreements are in place.
User organizations are responsible for verification and validation of User organization information submitted.
User organizations are responsible for development of an incident response plan at their sites in the event they are notified of an incident.
User organizations are responsible for reporting any issues encountered to ITD and for providing such assistance as is necessary to permit problem resolution.
User organizations are responsible for communicating compliance needs based on all applicable laws, requirements, and standards needed to operate.

Recommendations

Recommendation #1

ITD had core components listed in their Disaster Recovery that weren’t tested in either their DR testing or during any outages that occurred. ITD states Disaster Recovery of core ITD components are tested on a regular basis. ITD was not monitoring the core components to ensure testing was carried out on them all. Without adequate testing it is difficult to ensure recovery plans will work as intended.

We recommend ITD test disaster recovery of all their core components.

ITD Response:

Though ITD tests most of the core components two items have been identified as missing from DR Tests. ITD will work to implement testing procedures to include the identified components.

Recommendation #2

During our testing we noted 4 tapes that were listed as having been destroyed. One of those backup tapes was later found to still be in possession of the storage team. Also we found 60-70 hard drives that were to be destroyed locked in a cabinet. ITD stated they follow IRS Guidelines for tape and hard disk destruction. ITD didn't monitor these expired tapes/hard disk drives to ensure they were destroyed in a timely manner. A security risk could occur if the expired tapes/hard disk drives have sensitive information on them.

We recommend ITD destroy tapes/hard drives that have expired in a timely manner.

ITD Response:

ITD has procedures that address federal requirements for the destruction of physical media in place. ITD will adjust media protection policies to address the timeframe in which such media should be destroyed.

Recommendation #3

There are 46 active privileged accounts that have never been logged into. As stated in ITD's controls, new users and group memberships are authorized based on the role they will be filling within ITD. ITD failed to ensure that the privileged accounts were needed and to ensure that once they were setup the user logged in at least once to change the password. These accounts still have the default password and are not disabled after 90 days because ITD's process for disabling accounts doesn’t look at accounts never used.

We recommend ITD ensure employees need privileged accounts before setting them up and once setup ensure the account password is changed.

ITD Response:

ITD will edit the existing AD lockout script to include unused privileged accounts. The disabling of these accounts will trigger a review to determine if privilege rights are needed for these users.

Recommendation #4

Not all portable devices at ITD are encrypted. Devices should be encrypted so the data on them is protected. There is no process in place to verify that devices are encrypted. Unencrypted devices allow for unauthorized access to data.

We recommend ITD ensure all portable devices are encrypted.

ITD Response:

ITD will use the same methods used in this audit in order to check for compliance with encryption controls.

Recommendation #5

ITD has administrative groups that contain both privileged and non-privileged accounts. ITD States that privileged accounts are used for system administrative activities. ITD is transitioning to the use of privileged accounts and is still using some general accounts for admin until they work out all the issues and problems. Privileged accounts have greater security requirements, using general accounts for admin increases the security risk.

We recommend ITD ensure that only privileged accounts are used for admin activities.

ITD Response:

Once the transition of the privilege accounts has been completed ITD will review the groups used for privileged access and institute a group clean up and ongoing checks.

Recommendation #6

ITD currently allows employees access to the data centers who do not appear to require such access. ITD stated in their description of controls that access granted to restricted areas allows only authorized personnel within these areas. Currently ITD has too broad a definition of who should be authorized to accesses the data centers. Unneeded access to these restricted areas could cause security problems.

We recommend ITD review who has access to the data centers and ensure access is restricted to only employees who require such access.

ITD Response:

ITD does review access to the data centers. Per the recommendation ITD will further reduce the number of employees with access to the datacenters and maintain documentation such reviews have occurred.

Recommendation #7

Job-Related Training is not being done for all employees at ITD. ITD’s Personnel and Administrative Policies and Procedures Manual states ITD's goal is to provide training and development opportunities that: build and retain a skilled and effective workforce; improve organizational performance and maintain professional proficiency. ITD didn't monitor employee training to ensure employees received some job relate training. Employees may not be aware of the most current technological changes.

We recommend ITD monitor job-related training for employees to ensure training is provided to meet ITD's goals.

ITD Response:

ITD evaluates and provides for employee training needs as determined by the employee and their supervisor. While all training is monitored when the employees are sent to industry training classes, signup for online trainings, or college classes, there is no tracking on the more informal methods of training that are used. ITD will work to ensure all employee training is tracked through the ELM system.