Pursuant to the Information Technology Act of 2001, the Montana State Auditor's Office presents its plan for information technology for the period July 2016 through June 2021. This plan represents the Information Technology goals, objectives, and strategies of the of the State Auditor's Office and has been reviewed and approved by _____ Agency Head.

State of Montana

Commissioner of Securities and Insurance at the State Auditor's Office IT Strategic Plan 2016

Table of Contents

Executive Summary

The Montana Commissioner of Securities and Insurance (CSI), also known as the Montana State Auditor, is the chief regulator of Montana's insurance and securities industries. The Office of the Commissioner of Securities and Insurance, Montana State Auditor, is a criminal justice agency whose primary mission is to protect Montana's consumers through insurance and securities regulation.

CSI Information Technology department actively pursues innovative solutions to the agency's technology needs. Developing custom interfaces, providing stable infrastructure, and leveraging emerging technologies to advance the business objectives of CSI and the State of Montana.

Environment, Success, and Capabilities

The Commissioner of Security and Insurance Montana State Auditor (CSI) IT Department strives to provide technological solutions to meet the needs of CSI. Our primary purpose is to discover business processes and assist in developing or implementing solutions to meet the needs of these processes. The end result is a technological solution that lets CSI employees meet the needs of the people of Montana in an easier and more effective manner.

To be successful, CSI's IT department must be contemporary, flexible, and secure with the ability to respond to ever changing requirements. To enable and ensure that IT can meet expectations, continued emphasis is placed on ensuring a strong and secure technical infrastructure foundation through which all information technology systems, applications, and services are provided.

CSI has the following principles to develop and maintain consistent delivery of IT goods and services.

- Our IT decisions will align with CSI's strategic plan, including priorities, vision and goals.
- We will continually engage the agency staff as members of a team united to accomplish the agency's mission statement.
- We will identify issues, the level of complexity and escalate those issues to the appropriate resources as necessary.
- We will develop standardized policies and procedures for all users.
- We will ensure the IT department makes all resources available to all users as required.
- Current knowledge and skills are critical to IT's effectiveness in supporting agency staff and Montana's citizens

IT Contributions and Strategies

CSI is faced with major challenges and opportunities. These challenges and opportunities are caused by heightened expectations from not only CSI's staff, but also citizens and the business community who need to interact and conduct business with CSI. Utilizing modern capabilities, combined with the need to leverage and enhance limited staff resources, CSI will meet the needs of its employees and the expectations of the citizens of Montana. This strong and secure technical infrastructure foundation allows CSI to communicate effectively internally and externally throughout the agency and the community, and allows appropriate and secure access.

Information Security investments provide the means for this agency to protect itself and the citizens of Montana from those who would wish to cause harm. Security systems and practices are used to ensure the security and validity of information required for use in our role protecting citizens of the State of Montana.

In order to meet these challenges and opportunities, CSI's IT department will stay abreast of new technologies and innovative approaches.

• IT Principles

CSI maintains a number of foundational principles that have root in the Montana Information Technology Act to guide the work of our technology workforce. The following principles are what this strategic plan is built on.

- Resources and funding will be allocated to the IT projects that contribute the greatest net value and benefit to CSI stakeholders.
- Unwarranted duplication will be minimized by sharing data, IT infrastructure, systems, applications and IT services.
- IT will be used to provide a favorable business climate, improve government, protect individual privacy and protect the privacy of IT information.
- IT resources will be used in an organized, deliberative and cost-effective manner.
- IT systems will provide delivery channels that allow citizens to determine when, where, and how they interact with CSI.
- Mitigation of risks is a priority for protecting individual privacy and the privacy of IT systems information.
- Provide services in alignment to the ongoing needs and requirements of the Agency.
- Design solutions in support of expressed business needs; build these solutions in alignment with the availability, capacity and functionality needs of the Agency.
- Continually engaging agency staff as members of a team united to accomplish the agency's mission statement.

• IT Governance

The IT manager meets weekly with the Executive Staff (Tuesday's at 12pm) to ensure that technologies or services offered are in alignment with agency business goals and objectives.

CSI utilizes an IT Governance Committee which is comprised of the executive officers who review, approve, and make final decisions on matters in accordance with the agency strategic goals and initiatives. This group meets at a minimum quarterly to review progress and make continued recommendations on availability, security and continuity of IT services for the Agency as well as to share best practices and foster communication for the Agency.

• IT Financial Management

Agency IT costs are charged to a central IT cost center (Agency IT). Agency IT is primarily base budget funded with additional special projects funding requested during legislative sessions as needed.

- CSI has “OTO” appropriations dedicated to updating hardware approaching the end of its useful life--to absolutely essential or mandated changes.
- Designate systems as "legacy" and schedule their replacement. This approach will help focus investments toward the future rather than the present or past.
- Invest in education and training to ensure the technical staff in IT understand and can apply current and future technologies
- Investment in IT can never stop. As systems reach the end of life or as new technologies emerge that can enhance our current systems become more cost effective, we will always need to refresh and invest.

• IT Services and Processes

CSI’s IT Department provides in general, all levels of Information Technology related tools and services, consistently delivering the following to the Agency:

- Network and Infrastructure - server and infrastructure design and maintenance and document image and management solution design and deployment.
- Security - secure environment, data integrity, backup and recovery solutions, disaster recovery operations and plans. Risk management monitoring, user and application security.
- Data Management and Application Development – in-house development, design and support, maintaining, and enhancing the agency’s database and supported applications.
- Customized Software Solutions – Web development database application development.
- Desktop Support and maintenance – management of Agency’s desktops, network printers and scanner systems.

• IT Infrastructure, Staffing and Resources

CSI current infrastructure is comprised of a multi-server environment that services the entire agency’s data needs. This environment was designed with environmental and agency growth concerns in mind. CSI’s current backup environment has recently been updated to include redundancy which is hosted in the State of Montana Data Center. This allows for onsite backup with offsite redundancy which allows for a broader scope of disaster recovery options. CSI’s infrastructure has been engineered to meet the growing needs of the agency staff, while still maintaining costs at a lower threshold.

CSI currently has 4 FTE positions within their Information Technology Department. These positions include an IT manager, Database Analyst, Security/Network Officer, and a Computer Support Specialist.

- The **IT Manager** focus’ on the prioritization of agency projects, staffing requirements, and promotion of agency IT initiatives, document image and management solution design and deployment.
- The **Database Analyst** is responsible for in-house development, maintaining, and enhancing the agency’s database, supported applications.

- The **Security Officer** is responsible for ensuring a secure environment, data integrity, server and infrastructure design and maintenance and implement disaster recovery operations and plans.
- The **Computer Support Specialist** is responsible for assisting users with any desktop and application support

Each position is responsible for supporting the agency users with day-to-day operations while also focusing on supporting CSI systems in their respective specialized concentrations.

• Risks and Issues

Primary Risk	Probability	Impact	Mitigation Strategy
Staff retirements	Medium	High	The agency will develop a succession planning program and replacement plan when possible.
Difficulty of hiring qualified technical staff	High	High	Increase pay for positions most affected by this issue. Also would require adequate training, tools, and opportunities to refresh skills and develop new competencies
Security breach	Medium	High	Our agency has an active security program including, but not limited to, staff training and awareness, data encryption, and security policies.

• IT Goals and Objectives

- Provide safe and secure IT environments, security tools, and business processes that protect critical data and minimize the risk of interruptions.
- Implement IT security systems to accomplish Security Information and Event Management (SIEM) with automated alerting and reporting
- Provide balanced management of information and technology - Dedicated to providing effective systems that meet the needs of our Agency.
- Modernize critical Legacy technologies.
- Be flexible and responsive to changing priorities and requirements.
- Employee development- Support and provide opportunities for continuous improvement and development. Equip the IT department with the right tools and training as well as challenging and leveraging their skills and abilities to support our technology infrastructure and implement CSI's technology vision that training exists for the successful completion of all phases of the project lifecycle, from concept to completion.

• IT Projects

Item	Description
Project name	**Sales Force**
Project/program purpose and objectives	The vast majority of Securities filings are currently maintained on databases external to the SAO and by a for profit bank. This may be in violation of state law and is not consistent with best practices. The system needs to interface with SEC EDGAR Database, NASAA EFD, and BNYMELLON BLUE EXPRESS. In addition, by housing the data in the system, we will be able to provide a web interface for citizens of Montana to easily research potential investments.
Estimated start date	ASAP
Estimated cost	$60k implementation
Funding source - 1	
Funding source - 2	**Agency Budget**
Funding source - 3	
Annual Costs upon completion	$60 ongoing licensing
Item	**Description**
Project name	**CSI Legacy System Replacement**
Project/program purpose and objectives	This project is to replace a legacy system that supports both the Securities and Insurance divisions. The replacement system will be maintained on updated backend infrastructure and developed in industry standard application methods. The replacement system is currently being developed and documented to allow for future enhancements and integration for additional systems critical to CSI. By replacing the legacy system, it has provided a reliable platform for CSI staff to perform day-to-day operations critical to CSI's success and will completed by 12/31/2016.
Estimated start date	April 2014
Estimated cost	
Funding source - 1	**Agency Budget**
Funding source - 2	
Funding source - 3	
Annual Costs upon completion	

• Security and Business Continuity Programs

The Commissioner of Securities and Insurance has an agency information security management program that complies with §2-15-114, MCA and ITSD Information Security Programs policies and procedures with our adoption of the National Institute of Standards and Technology (NIST) Special Publication 800 series as a guide. This basic program attempts to align with SITSD's direction for an enterprise approach

to protect sensitive and critical information being housed and shared on state and/or external information assets or systems.

CSI's information security management program is challenged with limited resources and staff time. While IT staff continues to review alternatives and implement mitigation efforts, the level of acceptable risk is constantly challenged by the ever changing technology and associated risks from growing attacks.

As described in NIST SP 800-39, the agency established risk management policies and procedures to guide the agencies processes and services through the information technology lifecycle. This structure provides a programmatic approach to reducing the level of risk to an acceptable level, while ensuring legal and regulatory mandates are met in accordance with MCA §2-15-114.

The agency's program now fully includes the four components proposed by NIST, which interact with each other in a continuous improvement cycle. The four components are as follows:

- Risk Frame – Establishes the context for making risk-based decisions
- Risk Assessment – Addresses how the agency will assess risk within the context of the risk frame, identifying threats, harm, impact, vulnerabilities and likelihood of occurrence
- Risk Response – Addresses how the agency responds to risk once the level of risk is determined based on the results of the risk assessment; e.g., avoid, mitigate, accept risk, share or transfer;
- Risk Monitoring – Addresses how the agency monitors risk over time

By applying the NIST framework in developing its technical security program, CSI will reduce the risks that the agency is exposed to through the use of IT systems.

Current met objectives are;

- Develop and publish policies and procedures that are based on risk assessments.
- Conduct security awareness training.
- Develop a process for planning, implementing, evaluating, and documenting remedial actions;
- Develop procedures for detecting, reporting, and responding to security incidents; and
- Develop plans and procedures for continuity of operations.
- Conduct periodic risk assessments.

Current objectives still to be considered and completed;

- Conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls.
- Create and document security risk assessments of all existing systems in accordance with newly established agency policies.
- Implement SIEM/UTM systems for in-depth view and reporting of system and network status.

CSI has implemented all applicable ITSD information security policies as required or implemented new policies and procedures to improve upon or fill gaps in existing policies and practices. Our current goal is to establish annual review of all policies to;

- Run a gap analysis on business processes and fix or replace policies and procedures as required.
- Recognize gaps and risks in existing security management programs and identify and mitigate those discovered risks.
- Further expand upon the existing policies and procedures to graduate to a higher level of security (currently moderate for new systems in accordance with NIST SP800-53 R4) where possible to further mitigate future risks.

Continuity of Operations (COOP) Capability Program Description:

In April, 2012, CSI joined with the Montana Department of Administration's Security and Continuity Services (SCS) for the redevelopment of the agency's continuity of operations capabilities. SCS will provide the plans and structure for response and recovery capabilities at CSI, ensuring the continued performance of the essential functions of CSI.

CSI was an early participant in the COOP program and the use of Living Disaster Recovery Planning System (LDRPS) software, but since that initial involvement, the approach that SCS uses to help agencies has changed drastically. CSI has made updating its COOP plan a high priority in the agency's IT plan.

Updating the COOP plan involves two blocks of focus: completing the Business Continuity Plans (BCP) in two phases and working on specific activity plans, including Emergency Action Plans (EAP), Information System Contingency Plans (ISCP), Communications Plans, Incident Management Plans, and more.

CSI has currently completed the first phase of the LDRPS process and is currently working the DOA and SOS for establishing critical documents and retention periods. At this time all business processes have been documented with all required services and materials needed for those processes. CSI is ready to process state-wide COOP testing and approval of all plans by CSI and the governor with the rest of the state agencies.

Future COOP Program Plans

CSI IT staff have, with the cooperation and assistance of DOA continuity staff, coordinated and developed the Continuity of Operations (COOP) plans for each of the agencies business processes. Our goals for the future development and maintenance of these plans are as follows;

- Train more staff to develop and maintain existing COOP plans.
- Establish a review process to annually review each COOP plan with the business process owner for needed updates and changes.
- Test annually through exercises and drill, with the cooperation of DOA, the COOP plans and recovery process.

Public Records – Agency Records Management:

All electronic records will be retained and disposed of in accordance with general records retention schedules, agency records retention schedules, and/or federal retention requirement.

- Establish record management and record retention timelines with the Secretary of State.
- Information identified and recorded under the COOP Program tie into the Records Management Program and fulfill Information Security Management Program requirements. Integration of these three programs is critical to the confidentiality, integrity, and availability of information associated with each program.

13. Planned IT Expenditures

	FY2016	FY2017	FY2018	FY2019	FY2020	FY2021
IT personal services	371,900	370,500	380,000	389,000	399,000	409,000
IT operating expenses	232,000	255,000	281,000	309,000	374,000	350,000
IT initiatives						
Other						
Total	603,900	625,500	661,000	698,000	773,000	759,000

14. Administrative Information

IT strategy and Plan Owner:

Name: The Commissioner of Securities and Insurance, Montana State Auditor
Telephone Number: (406) 444-2040
Email Address: Contact us on our website at http://csimt.gov/contact/

Information Technology Manager:

Name: Glynis Gibson
Telephone Number: (406) 444-3517
Email Address: gegibson@mt.gov

Senior Database Administrator:

Name: Ken Kops
Telephone Number: (406) 444-5787
Email Address: kkops@mt.gov

Information Security Officer:

Name:
Telephone Number:
Email Address: