State of Montana

Commissioner of Securities and Insurance at the State Auditor's Office IT Strategic Plan 2014

Table of Contents

1. Executive Summary

The Montana Commissioner of Securities and Insurance (CSI), also known as the 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 IT Staff 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 the CSI and the State of Montana.

2. Environment, Success, and Capabilities

A natural or other disaster may require an extraordinary response by the Office of the Commissioner of Securities and Insurance (CSI). In the event of such a disaster, CSI must respond quickly and effectively to meet the insurance needs of Montana's citizens, and coordinate CSI's resources with other state agencies in mitigating the effects of the disaster. By responding in an appropriate, effective and comprehensive manner, CSI can help ensure that the citizens of Montana are provided a coordinated response by all accountable parties.

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 guide the department to develop and maintain consistent delivery of IT goods and services.

- We will balance innovation with stability and reliability.
- 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 seek information and education regarding new technologies relevant to the user's job requirements.
- We will develop standardized policies and procedures for all users.
- We will ensure the IT department makes all resources available to all users in a non-discriminatory mode.

3. IT Contributions and Strategies

CSI is faced with major challenges and opportunities. These challenges and opportunities are caused by heightened expectations from not only the 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 necessary to accomplish the work. 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. Emphasis is also placed on processes to ensure that IT projects are managed consistently through proper levels of oversight and tracking.

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

4. IT Principles

CSI maintains a number of foundational principles that are in line with SITSD 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

5. IT Governance

The IT director meets weekly with the Deputy Commissioner 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 quarterly to review progress and make continued recommendations on availability, security and continuity of IT services for the Agency.

6. 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 "legacy systems" hardware and software 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.

7. IT Services and Processes

CSI’s IT Department provides in general, all levels of Information Technology related goods 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.
- 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 – management of Agency’s desktops, network printers and scanner systems.
- Resource Management – Measuring CSI’s IT capability and infrastructure to current and future business requirements.

8. IT Infrastructure, Staffing and Resources

CSI current infrastructure is comprised of a clustered virtual 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 5 FTE positions within one (1) Information Technology (IT) Bureau. These positions include an IT manager, Database Analyst, Security Officer, Network Engineer, and a Computer Support Specialist.

- The **IT Manager** focus' on the prioritization of agency projects, staffing requirements, and promotion of agency IT initiatives.
- The **Database Analyst** is responsible for in-house development, maintaining, and enhancing the agency's database and supported applications.
- The **Security Officer** is responsible for ensuring a secure environment, data integrity, and implement disaster recovery operations and plans.
- The **Network Engineer** is responsible for server and infrastructure design and maintenance and document image and management solution design and deployment.
- 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.

9. 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.
Staff Turnover	Medium	High	The agency needs a workforce with the necessary skillsets to support modern and emerging technologies.
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.

10. 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.
- 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.
- Strive every day to make the most efficient and effective use of the resources and funds we have available.
- Employee development- Support and provide opportunities for continuous improvement and development. Ensure CSI's IT's department has the knowledge and skills to support our technology infrastructure and implement CSI's technology vision and that training exists for the successful completion of all phases of the project lifecycle, from concept to completion
- Mobile Data Management – Establish mobile strategies to leverage mobile solutions to improve overall access to information and services offered.

11. IT Projects

Item	Description
Project name	**CSI Document Imaging and Management**
Project/program purpose and objectives	The implementation of document imaging and management is a critical business function to maintain a consistent and reliable source for agency staff to assist Security and Insurance industry customers with requests. Migrating from the legacy system will provide for limited risk in loss of technical expertise and provide for enhanced document retention policy assurance. The document management will allow for CSI to remain in compliance with state and federal laws in regards to document retention. The new system will allow for additional features which include document access security, disaster recovery, and consistent and reliable data capture. This project is funded through a legislative appropriations granted in session 2013.
Estimated start date	In progress
Estimated cost	
Funding source - 1	**2013 Legislative Appropriations**
Funding source - 2	**Agency annual budget**
Funding source - 3	
Annual Costs upon completion	**$164,207**
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 will be developed and documented to allow for future enhancements and integration for additional systems critical to CSI. Replacing the legacy system will provide for a reliable platform for CSI staff to perform day-to-day operations critical to CSI's success. The funding for the Legacy Replacement was granted by 2013 Legislation Appropriations.
Estimated start date	April 2014
Estimated cost	
Funding source - 1	**2013 Legislative Appropriations**
Funding source - 2	**Agency Budget**
Funding source - 3	
Annual Costs upon completion	

12. 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 ITSD'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. IT staff has identified specific vulnerabilities that require restructure or new equipment.
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, the 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.

Current objectives still to be considered and completed;

- Conduct periodic assessments of risks.
- 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.

The 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.
- Establish mitigation procedures for legacy systems to ensure they meet the moderate level of security required by ITSD and NIST SP800-53 R4 where possible.

Continuity of Operations (COOP) Capability Program Description:

In April, 2012, the 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 the CSI, ensuring the continued performance of the essential functions of the 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. The 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.

The 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. Our current goals are to;

- Establish ISCP plans for all current systems by the end of 2014 and integrate them with the agencies completed EAP.
- Establish record management and record retention timelines with the Secretary of State.

The CSI expects to be ready to process state-wide COOP testing and approval of all plans by the CSI and the governor with the rest of the state agencies.

Information identified and recorded under the COOP structure can 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.

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 processes.

13. Planned IT Expenditures

	FY2014	FY2015	FY2016	FY2017	FY2018	FY2019
IT personal services	425,742	431,377	436,645	436,645	436,645	436,645
IT operating expenses	280,500	300,000	320,000	335,000	350,000	350,000
IT initiatives	13,475	13,475	13,475	14,149	14,149	14,149
Other						
Total	719,717	744,852	770,120	785,794	800,794	800,794

14. Administrative Information

IT strategy and Plan Owner:

Name: The Commissioner of Securities and Insurance, Montana State Auditor
Telephone Number: 444-2040
Email Address: Contact us on our website at http://www.csi.mt.gov/contact.asp

Information Technology Manager:

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

Network Analyst:

Name: Ashley Downing
Telephone Number: 444-9773
Email Address: adowning@mt.gov

Information Security Manager:

Name: Josh Tuman
Telephone Number: 444-5233
Email Address: JTuman@mt.gov