

CONFIDENTIAL

DRAFT CONFIDENTIAL

DRAFT CONFIDENTIAL

DRAFT CONFIDENTIAL

DRAFT CONFIDENTIAL

DRAFT CONFIDENTIAL

DRAFT CONFIDENTIAL

Function	Major Policy Objective	Type	Policy Requirements	Coresponding NIST Control Objective	Assessor Notes	(%) Complete
<b>Identify</b>	<b>Identify Function</b>					<b>81</b>
1.1	Maintain an inventory of information systems components. Inventory of systems is conducted annually and reviewed for any unauthorized components. Unauthorized components are removed.	Identify Function	The State of Montana develops and maintains an inventory of its information systems.	CM-8, PM-5	<i>Processes are not complete for ensuring a comprehensive inventory of information system components is complete for each agency information system. Although, a scattered inventory of information systems is maintained.</i>	20
1.2	Map organizational communication and data flows	Identify Function	1.2.1 - Approve flows of information between information systems	AC-4	<i>Approved authorizations for controlling the flow of between interconnected systems is not currently evidenced.</i>	0
			1.2.2 - Require an Interconnection Security Agreement for all information systems directly connected to external systems	CA-3	<i>Interconnection Security Agreements are complete and updated for connections to external information systems.</i>	100
			1.2.3 - Each State information system has a security plan that outlines the connections with other information systems.	CA-3	<i>The system security plans outline connections with other information systems e.g., (SAN, backup, and audit aggregation server)</i>	100
			1.2.4 - The State agency employs a permit-by-documented request (exception) policy for allowing agency and other information systems to connect to external information systems.	CA-3	<i>The agency employs a permit-by-exception policy for information systems.</i>	100
			1.2.5 - The State agency ensures that all internal connection for an information system are documented within the system security plan.	CA-9	<i>Internal connections for agency information systems are documented within their respective system security plans.</i>	100
			1.3.1 - State agencies ensure compliance with access requirements for information systems.	AC-20	<i>Federated access controls are employed in the information systems. The agency has not established terms and conditions, consistent with any trust relationships established with other organizations, owning, operating, and/or maintaining external information systems, allowing authorized individuals to access the information system from the external information systems.</i>	0

1.3	The State agency maintains agreements with external entities when using external information systems to use, process, store, or transmit state data	Identify Function	1.3.2 - The State agency requires that providers of external information system services comply with organizational information security requirements and employ appropriate security in accordance with applicable state laws, Executive Orders, policies, standards, and guidance.	SA-9	<i>State of Montana - Department of Administration requires that external information system services employ, as part of the RFP review/granting process, enterprise-defined security controls in accordance with applicable state laws, Executive Orders, policies, standards, and guidance.</i>	100
			1.3.3 - The State agency defines and documents State of Montana oversight and user roles and responsibilities with regard to external information systems.	SA-9, PL-4	<i>The system security plans defines both oversight and user's roles and responsibilities in connection to external information system.</i>	100
			1.3.4 - The State agency monitors security control compliance by external service providers.	SA-9	<i>The agency requires external service providers demonstrate security control compliance through assessments and attestations.</i>	100
			1.3.5 - The State agency requires provider of information system services to identify the functions, ports, protocols, and other services required for the use of such services	SA-9	<i>Required system security plans document the functions, ports, protocols, and other services for the user of the information system.</i>	100
1.4	The State agency establishes cybersecurity roles and responsibilities for the workforce and third-party stakeholders (e.g., suppliers, customers, and partners).	Identify Function	The State agency establishes cybersecurity roles and responsibilities for the workforce and third-party stakeholders (e.g., suppliers, customers, and partners).	PS-7, SA-3	<i>The agency, within both policy objectives and system security plans, define cybersecurity roles and responsibilities for both internal employees and external partners.</i>	100
1.5	The State agency establishes dependencies, critical functions, and requirements, for delivery of critical services.	Identify Function	The State agency establishes dependencies, critical functions, and requirements, for delivery of critical services.	CP-2	<i>The agency does not identify critical information system assets supporting essential mission and business functions within a contingency plan. However, some critical services are defined within the COOP and ISIRT manuals.</i>	20
			1.6.1 - State agencies establish and maintain coordination and alignment of information security roles and responsibilities with internal roles and external partners	1 - controls from all families (except PM-1)	<i>State policy templates define security roles and responsibilities. Appendix B (Security Roles and Responsibilities) provides enterprise level granularity. Coordination with internal roles and external partners is defined within system security plans.</i>	100

1.6	The State agency establishes and maintains information security policies	Identify Function	1.6.2 - Legal and regulatory requirements regarding information security, including privacy and civil liberties obligations, are understood and managed.	1 - controls from all families (except PM-1)	<i>The POL-Information Security Policy is based on legal and regulatory requirements for State agencies as defined with Montana Code. Additionally, privacy and civil liberty obligations, including prohibited and allowed disclosures for various data types, are addressed within the POL-Data Classification Policy.</i>	100
			1.6.3 - State agencies ensure that governance and risk management process address information security risks.	PM-9, PM-11	<i>The agency has developed a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems.</i>	100
1.7	The State agency identifies and documents asset vulnerabilities	Identify Function	1.7.1.1 - The State agency obtains, protects as required, and making available to authorized personnel, administrator documentation for the information system that describes secure configuration, installation, and operation of the information system.	SA-5	<i>System administrators and developers have access to documentation that details secure configuration, installation, and operation of the information system from vendor sources. These documents are typically produced during the procurement of the information system.</i>	100
			1.7.1.2 - The State agency obtains, protects as required, and making available to authorized personnel, administrator documentation for the information system that describes effective use and maintenance of security features/functions.	SA-5	<i>System administrators and developers have access to documentation that details effective use and maintenance of security features/functions. These documents are typically produced during the procurement of the information system.</i>	100
			1.7.1.3 - The State agency obtains, protects as required, and making available to authorized personnel, administrator documentation for the information system that describes known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.	SA-5	<i>System administrators and developers are not provided ongoing vulnerability information regarding configuration and use of administrative functions. MS-ISAC and CIS sources are available for providing this information to appropriate personnel. However, critical vulnerabilities and configuration guidance is not disseminated on an ongoing basis.</i>	20

1.7	The State agency identifies and documents asset vulnerabilities	Identify Function	1.7.2.1 - The State agency obtains, protects as required, and making available to authorized personnel, user documentation for the information system that describes user-accessible security features/functions and how to effectively use those security features/functions	SA-5	<i>Users have access to documentation that details user-accessible security functions/mechanisms and how to effectively use those functions/mechanisms.</i>	100
			1.7.2.2 - The State agency obtains, protects as required, and making available to authorized personnel, user documentation for the information system that describes methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.	SA-5	<i>Users have access to documentation that describes methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.</i>	100
			1.7.2.3 - The State agency obtains, protects as required, and making available to authorized user personnel, user documentation for the information system that describes user responsibilities in maintaining the security of the information and information system.	SA-5	<i>Users have access to documentation that describes user responsibilities in maintaining the security of the system, component, or service.</i>	20
			1.7.3 - The State agency documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	SA-5	<i>Users have access to documentation that details user-accessible security functions/mechanisms and how to effectively use those functions/mechanisms.</i>	100
			1.7.4 - The State agency protects documentation as required in accordance with the risk management strategy.	SA-5	<i>Users have access to documentation that describes methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.</i>	100
			1.7.5 - The State agency scans for vulnerabilities in information systems and hosted applications annually and when new vulnerabilities potentially affect the system/applications are identified and reported.	RA-5	<i>The State agency has not defined the frequency for conducting vulnerability scans on the information systems and hosted applications.</i>	0
			1.7.6.1 - The State agency employs vulnerability scanning tools and techniques that promote interoperability among tools and automating parts of the vulnerability management process by using standards for enumerating platforms, software flaws, and improper configurations.	RA-5	<i>The State agency utilizes Tenable "Nessus" Security Center that promotes interoperability among tools and automates parts of the vulnerability management process by enumerating platforms, software flaws, and improper configurations.</i>	100

1.7	The State agency identifies and documents asset vulnerabilities
-----	-----------------------------------------------------------------

Identify Function

1.7.6.2. - The State agency employs vulnerability scanning tools and techniques that promote interoperability among tools and automating parts of the vulnerability management process by using standards for formatting and making transparent, checklists and test procedures	RA-5	<i>The State agency utilizes Tenable "Nessus" Security Center that promotes interoperability among tools and automates parts of the vulnerability management process by formatting and making transparent, checklists, and test procedures.</i>	100
1.7.6.3. - The State agency employs vulnerability scanning tools and techniques that promote interoperability among tools and automating parts of the vulnerability management process by using standards for measuring vulnerability impact.	RA-5	<i>The State agency utilizes Tenable "Nessus" Security Center that promotes interoperability among tools and automates parts of the vulnerability management process by using standards for measuring vulnerability impact.</i>	100
1.7.7. - The State agency analyzes vulnerability scan reports and results from security control assessments.	RA-5	<i>The State agency utilizes Tenable "Nessus" Security Center for the creation of vulnerability scan reports. These vulnerability scan reports and security control assessments provide help in analysis.</i>	100
1.7.8. - The State agency remediates critical vulnerabilities within thirty (30) business days in accordance with organizational assessment of risk.	RA-5	<i>The State agency performs an organizational assessment of risk and remediates critical vulnerabilities within 30 days.</i>	100
1.7.9. - The State agency shares information obtained from the vulnerability scanning process and security control assessments with designated personnel to help eliminate similar vulnerabilities in other information systems.	RA-5	<i>The State agency disseminates vulnerability scanning information and security control assessments with designated personnel to aid in the elimination of similar vulnerabilities.</i>	100
1.7.10. - The State agency employs a vulnerability scanning tool that automates vulnerability list updates at least weekly, prior to a new scan, and when new vulnerabilities are identified and reported.	RA-5	<i>The State agency utilizes Tenable "Nessus" Security Center that automates vulnerability list updates at least weekly.</i>	100
1.7.11. - The State agency authorizes privileged access for vulnerability scanning.	RA-5	<i>Privileged accounts are approved for users employing Tenable "Nessus" Security Center.</i>	100

			1.7.12.1. - The State agency requires that information system developers/integrators create and implement a security test evaluation plan.	SA-11	<i>The state agency does not, through a a security test and evaluation plan: 1. Define the depth of testing/evaluation to be performed by the developer of the information system, system component, or information system service. 2. Define the coverage of testing/evaluation to be performed by the developer of the information system, system component, or information system service. 3. Requires the developer of the information system, system component, or information system server to perform one or more of the following testing/evaluation at the agency-defined depth and coverage: unit testing/evaluation, integration testing/evaluation, system testing/evaluation, and/or regression testing/evaluation.</i>	0
			1.7.12.2. - The State agency requires that information system developers/integrators implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.	SA-11	<i>The State agency does not employ a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process.</i>	0
			1.7.12.3. - The State agency documents the results of the security testing/evaluation and flaw remediation processes.	SA-11	<i>The State agency does document the results of the security testing/evaluation and flaw remediation processes.</i>	0
			1.8.1. - The State agency receives security alerts, advisories, and directives that originate from designated trusted external organizations.	SI-5	<i>The State of Montana receives security alerts from trusted entities (e.g., MS-ISAC and the Center for Internet Security).</i>	100
			1.8.2. - The State agency communicates security alerts, advisories, and directives on an ongoing basis.	SI-5	<i>The State of Montana communicates security alerts, advisories, and directives are communicated on an ongoing basis.</i>	100
			1.8.3. - The State agency generates internal security alerts, advisories, and directives as deemed necessary.	SI-5	<i>The State of Montana generates internal security alerts, advisories, and directives as deemed necessary.</i>	100

1.8	Receive security alerts, advisories, and directives	Identify Function	1.8.4. - The State agency are disseminated to appropriate entity/agency security contract for their use and distribution.	SI-5	<i>The State of Montana disseminates security alerts, advisories, and directives to appropriate entity/agency security contracts for their use and distribution.</i>	100
			1.8.5. - The State agency utilizes security alerts, advisories, and directives to implement security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	SI-5	<i>The State agency consults with the State enterprise entity that communicates security alerts, advisories, and directives in accordance with established time frames, or notifies the State enterprise entity of the degree of noncompliance.</i>	100
			1.8.6. - The State agency that receives security alerts, advisories, and directives that are used to facilitate ongoing security education and training for organizational personnel.	PM-15	<i>The State agency utilizes security alerts, advisories, and directives are used to facilitate ongoing security education and training for organizational personnel.</i>	100
			1.8.7. - The State agency maintains currency with recommended security practices, techniques, and technologies.	PM-15	<i>The State agency maintains currency with recommended security practices, techniques, and technologies.</i>	100
			1.8.8. - The State agency shares current security-related information including threats, vulnerabilities, and incidents.	PM-15	<i>The State agency communicates with other approved entities threats, vulnerabilities, and incidents.</i>	100
			1.8.9. - The State agency utilizes security alerts, advisories, and directives that are used to implement a threat awareness program that includes a cross-organization information-sharing capability.	PM-16	<i>The State agency cooperates with the State enterprise entity towards the implementation of a cross-organizational threat awareness program.</i>	100
1.9	The State agency conducts risk assessments	Identify Function	1.9.1. The State agency conducts risk assessments that include the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information it processes, stores, or transmits.	RA-3	<i>The State agency conducts risk assessments that include the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems and the information it processes, stores, or transmits.</i>	100
			1.9.2. - The State agency conducts risk assessments that include documentation of the risk assessment results in a risk assessment report.	RA-3	<i>The State agency conducts risk assessments that include documentation of the risk assessment results in a risk assessment report.</i>	100
			1.9.3. - The State agency conducts risk assessments that include annual review of the risk assessment results.	RA-3	<i>The State agency conducts risk assessments that include annual review of the risk assessment results.</i>	100

			1.9.4. - The State agency conducts risk assessments that include annual updates of whenever there are significant changes to information systems or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may affect the security state of the system.	RA-3	<i>The State agency conducts risk assessments that include annual updates of whenever there are significant changes to information systems or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may affect the security state of the system.</i>	100
1.10	The State agency establishes security categorizations	Identify Function	1.10.1. - The State agency establishes security categorizations that are in accordance with applicable state laws, Executive Orders, directives, policies, standards, and guidance.	RA-2	<i>The State agency establishes security categorizations that are in accordance with applicable state laws, Executive Orders, directives, policies, standards, and guidance.</i>	100
			1.10.2. - The State agency establishes security categorizations that are documented within the security plan for each information system.	RA-2	<i>The State agency establishes security categorizations that are documented within the security plan for each information system.</i>	100
			1.10.3. - The State agency establishes security categorizations that ensures the authorizing official or designated representative reviews and approves of the security categorization decision.	RA-2	<i>The State agency establishes security categorizations that ensures the authorizing official or designated representative reviews and approves of the security categorization decision.</i>	100
1.11	The State agency implements a plans of action and milestones for the security program and the associated organizational information systems	Identify Function	1.11.1. - The State agency implements a plans of action and milestones for the security program and the associated organizational information systems are developed and maintained.	PM-4	<i>The State agency implements a plans of action and milestones for the security program and the associated organizational information systems are developed and maintained.</i>	100
			1.11.2. - The State agency implements a plans of action and milestones for the security program and the associated organizational information systems contain documentation of the remedial information actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the State.	PM-4	<i>The State agency implements a plans of action and milestones for the security program and the associated organizational information systems contain documentation of the remedial information actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the State.</i>	100

			1.11.3. - The State agency implements a plans of action and milestones for the security program and the associated organizational information systems are reported in manner consistent with State of Montana (OMB FISMA) requirements.	PM-4	<i>The State agency implements a plans of action and milestones for the security program and the associated organizational information systems are reported in manner consistent with State of Montana (OMB FISMA) requirements.</i>	100
1.12	The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems.	Identify Function	1.12.1 - The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes establishing and communicating priorities for organizational mission, objectives, and activities.	PM-9	<i>The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes establishing and communicating priorities for organizational mission, objectives, and activities.</i>	100
			1.12.2 - The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes organizational risk tolerance that is clearly expressed and communicated.	PM-9	<i>The State agency determines and clearly expresses and communicates organizational risk tolerance.</i>	100
			1.12.3 - The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes a definition of mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State.	PM-9	<i>The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes a definition of mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the State.</i>	100

			<p>1.12.4 - The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes a determination of information protection needs arising from the defined mission/business processes and revision to the processes as necessary, until and acheive set of protection needs is obtained.</p>	PM-9	<i>The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes a determination of information protection needs arising from the defined mission/business processes and revision to the processes as necessary, until and acheive set of protection needs is obtained.</i>	100
			<p>1.12.3 - The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes development, documenation, and updating of critrication infrastructure and key resources protection plan.</p>	PM-9	<i>The State agency develops and implements a comprehensive and consistent strategy to manage risk to organizational operations and assets, individuals, other organizations, and the State associated with the operation and use of information systems that includes development, documenation, and updating of critrication infrastructure and key resources protection plan.</i>	100
<b>Protect</b>		<b>Protect Function</b>				<b>65</b>
			<p>2.1.1 - The State agency provides unique identification and authentication to information systems.</p>	IA-2, IA-3, IA-8	<i>Evidence exixsts that organizational processes are in effect for uniquely identifying and authenticating users and devices.</i>	100
			<p>2.1.2 - The State agency employs the use of multifactor authentication for access to privileged accounts.</p>	IA-2	<i>The State agency does not employ multifactor authentication mechanisms for privileged network user accounts.</i>	0

2.1	Manage identities and credentials for authorized devices and users	Protect Function	2.1.3 - The State agency utilizes unique identification and authentication to all network attached devices compatible with the 802.1x protocol prior to establishing a network connection.	IA-3	<i>Prior to establishing a network connection, the State agency employs automated mechanisms for supporting and/or implementing device identification and authentication capability. The organizational authentication solution is employed (IEEE 802.1x) to authenticate devices on local and/or wide area networks. When a device first attaches to a network, the client supplicant software on that device transmits an authentication request to the authenticator, which is usually a network switch. The switch recognizes the request and is preconfigured to forward it to the appropriate authentication server. The authentication server makes its determination and transmits an "allow" or "deny" message back to the switch. Finally.</i>	100
			2.1.4.1 - The State agency provides unique information system identifiers (UserID)s by requesting the identifier from SITSID.	IA-4	<i>The State agency utilizes SITSID for provisioning unique system identifiers.</i>	100
			1.2.5 - The State agency ensures that all internal connection for an information system are documented within the system security plan.	CA-9	<i>Internal connections for agency information systems are documented within their respective system security plans.</i>	100
<b>Recover</b>		<b>Recovery Function</b>				<b>70</b>
			5.1.1 - Adherence to established contingency planning requirements through the POL- State Government Continuity Program is conducted.	CP-1	<i>The contingency plan does not currently reflect the requirements established by the POL-State Government Continuity Program.</i>	0
			5.1.2 - Essential mission and business functions and associated contingency requirements are defined.	CP-2	<i>The contingency plan does not define essential mission and business functions.</i>	0
			5.1.3 - Maintaining essential mission and business functions despite disruption, compromise, or failure are addressed	CP-2	<i>The contingency plan does not provide details related to maintaining essential mission/business functions if a major incident were to occur.</i>	0
			5.1.4 - Eventual, full information system restoration, without deterioration, of the security safeguards originally planned and implemented is addressed	CP-2	<i>Restoration of information system with security safeguards are not being met.</i>	10
			5.1.5 - Recovery objectives, restoration priorities, and metrics are addressed.	CP-2	<i>Recovery objectives and restoration priorities are established with metrics.</i>	100

5.1	Develop contingency plans and procedures for each information system	Recovery Function		CP-2	<i>Role and responsibilities are sufficiently documented.</i>	100
			5.1.7 - Distribution of copies of the contingency plan to key contingency personnel is conducted.	CP-2	<i>Copies of the contingency plan are distributed to appropriate personnel.</i>	100
			5.1.8 - Contingency planning activities with incident handling activities are conducted.	CP-2	<i>Tabletop exercises are conducted with incident handling capabilities.</i>	100
			5.1.9 - Review of the contingency plan for the information systems are conducted annually.	CP-2	<i>A review of the contingency plan occurs at least once a year and the contingency plan contains a revision date.</i>	100
			5.1.10 - Revision of the contingency plan to address changes to State governance, information system, or environment of operation and problems encountered during implementation, execution, or testing is demonstrated.	CP-2	<i>The contingency plan does not reflect changes to state policy and move to the new server environment. However, these changes have fallen between revision periods.</i>	50
			5.1.11 - Communication of contingency plan changes to key contingency personnel occurs.	CP-2	<i>The contingency plan changes are communicated to key personnel.</i>	100
			5.1.12 - Review and approval by the appropriate agency authorizing official is performed.	CP-2	<i>Review and authorization of the contingency plan is conducted by the authorizing official.</i>	100
			5.1.13 - Contingency plan protection mechanisms from unauthorized disclosure and modification is demonstrated.	CP-2	<i>The contingency plan is located on a SharePoint drive with appropriate access controls applied.</i>	100
5.2	Conduct appropriate training through the state continuity program and other training opportunities.	Recovery Function	The State of Montana conducts appropriate training through the state continuity program.	CP-3	<i>Tabletop exercises are conducted with incident handling capabilities.</i>	100
5.3	Conduct appropriate contingency plan testing through the state continuity program, agency continuity program, SITSD, and/or other testing programs.	Recovery Function	The State of Montana conducts appropriate contingency plan testing through the state continuity program.	CP-4	<i>Sufficient testing of the contingency plan has not been conducted at the time of assessment.</i>	0
5.4	Maintain an offsite storage site to be in place and used for essential business functions.	Recovery Function	The State of Montana requires that an offsite storage site be in place and used for essential business functions.	CP-6	<i>An offsite storage site is currently in use for essential business functions.</i>	100
5.5	Ensure an alternative processing site is in place and can be used for essential business functions	Recovery Function	The State of Montana requires that an alternative processing site be in place and used for essential business functions.	CP-7	<i>Remote access capabilities along with alternative sites can be utilized as alternative processing sites.</i>	100
5.6	Ensure alternate telecommunication services are available for essential mission and business functions at primary and alternate processing storage sites.	Recovery Function	The State of Montana has alternate telecommunication services for essential mission and business functions at primary and alternate processing and storage sites.	CP-8	<i>Redundant telecommunication services exist to support essential mission/business functions at the primary and alternate processing and storage sites.</i>	100
5.7	Conduct backups of user-level and system-level information contained in the information system as defined by the data owner.	Recovery Function	The State of Montana conducts backups of user-level and system-level information contained in the information system as defined by the data owner. Documentation is reviewed and tested annually.	CP-9	<i>User and system level information is backed up. However, this information is not validated by the data owner and no documentation or testing has been conducted at the time of assessment.</i>	50

5.8	Provide for the recovery and reconstitution of systems, including transaction recovery, to a known state after disruption, compromise, or failure.	Recovery Function	The State of Montana provides for the recovery and reconstitution of systems to a known state.	CP-10	No evidence that reconstitution to a known state has been tested. However, documentation does exist of backup information.	75
5.8	Provide for the recovery and reconstitution of systems, including transaction recovery, to a known state after disruption, compromise, or failure.	Recovery Function	The State of Montana provides for the recovery and reconstitution of systems to a known state.	CP-10	No evidence that reconstitution to a known state has been tested. However, documentation does exist of backup information.	75
<b>Respond</b>	<b>Respond Function</b>					<b>94</b>
4.1	Develop, document, and disseminate incident response process.	Respond Function	4.1.1 - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	IR-1	The incident response plan does not specifically address coordination among organizational entities and does not contain reporting compliance information for external entities/partners.	60
		Respond Function	4.1.2 - Establishes reviews and updates to incident response policy and procedures within two years of last review.	IR-1	The incident response policy and procedures document has a revision date of July of 2015.	100
		Respond Function	4.1.3 - Incident response policy and procedures follow the National Incident Management System (NIMS) guidance.	IR-1	There is no specific guidance on how to follow NIMS within the policy and procedures.	0
4.2	Conduct training of personnel in their incident response roles and responsibilities on an annual basis.	Respond Function	The agency conducts applicable training of personnel detailing their roles and responsibilities for incident response on an annual basis.	IR-2	Annual training is conducted with the ISIRT manual with individuals that have roles/responsibilities for incident response related activities.	100
4.3	Conduct tests and/or exercises for the incident response capability annually using designed tabletop and real-life scenarios/exercises to determine the incident response effectiveness and documents the results. These tests may be coordinated with other groups or plans such as Business Continuity, Disaster Recovery, Continuity of Operations, Crisis Communications, Critical Infrastructure, Emergency Action, etc.	Respond Function	The agency conducts tests of the ISIRT in coordination with the LDRPS system and usage of the COOP.	IR-3	Annual exercises are conducted with the ISIRT manual in coordination with the LDRPS systems and the COOP.	100
4.4	Implement an incident handling capability for security incidents.	Respond Function	4.4.1 - Includes preparation, detection and analysis, containment, eradication, and recovery.	IR-4	The ISIRT manual contains specific direction on preparation, detection and analysis, containment, eradication, and recovery.	100
		Respond Function	4.4.2 - Coordinates incident handling activities with contingency planning activities.	IR-4	The ISIRT manual contains incident handling activities that are in coordination with contingency planning activities.	100

		Respond Function	4.4.3 - Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	IR-4	<i>Lessons learned from ongoing incident handling activities are incorporated into the changes in the ISIRT.</i>	100
		Respond Function	4.4.4 - Employs automated mechanisms to support the incident handling process.	IR-4(1)	<i>Utilization of POB is used for automated incident handling processes.</i>	100
4.5	Track and document information system security incidents.	Respond Function	The agency tracks and documents information system security incidents.	IR-5	<i>Utilization of POB is used for tracking and documenting security incidents is demonstrated.</i>	100
4.6	Implement an incident reporting requirement for personnel	Respond Function	4.6.1 - Ensures incidents are reported to the Service Desk within 24 hours of occurrence.	IR-6	<i>Suspected security incidents are always reported to the Service Desk.</i>	100
		Respond Function	4.6.2 - SITSD reports enterprise security incident information to Executive staff, the Information Technology Managers Council, Information Security Advisory Council, and the Legislative Audit Division on a monthly basis.	IR-6	<i>Reports are generated on major incidents are reported to the various entities on a monthly basis.</i>	100
		Respond Function	4.6.3 - Automated mechanisms are utilized to assist in the reporting of security incidents.	IR-6	<i>POB is utilized to aggregate and report on security incidents.</i>	100
4.7	Utilize the SITSD Service Desk, SITSD Information Systems Security Office, National Guard, MS-ISAC, Fusion Center and State Risk Management and Tort Claims Division as an incident response support resource.	Respond Function	4.7.1 - Outside entities are utilized by the agency for support and handling of incidents.	IR-7	<i>The agency reaches out to outside entities for assistance in handling incidents.</i>	100
		Respond Function	4.7.2 - Automated mechanisms are employed to increase the availability of incident response related information and support.	IR-7	<i>Automated systems such as POB and Albert sensors are employed to increase availability and support services for incident response.</i>	100
		Respond Function	4.8.1 - Provides a roadmap for implementing its incident response capability.	IR-8	<i>Suspected security incidents are always reported to the Service Desk.</i>	100

4.8

Develop an ISIRT (Information Systems Incident Response Team) Manual

Respond Function	4.8.2 - Describes the structure and organization of the incident response capability.	IR-8	<i>The structure and organization of incident response capability is described.</i>	100
Respond Function	4.8.3 - Provides a high-level approach for how the incident response capability fits into agency processes.	IR-8	<i>Agency processes integrate the incident response capability.</i>	100
Respond Function	4.8.4 - Meets the requirements of mission, size, structure, and functions of the agency.	IR-8	<i>The ISIRT manual addresses the unique agency requirements.</i>	100
Respond Function	4.8.5 - Defines reportable incidents.	IR-8	<i>A classification of reportable incidents is established.</i>	100
Respond Function	4.8.6 - Provides metrics for measuring the incident response capability for the agency.	IR-8	<i>Metrics are established by the ISIRT for established reporting requirements.</i>	100
Respond Function	4.8.7 - Defines the resources and management support needed to effectively maintain and mature an incident response capability;	IR-8	<i>Resources and management support for the ISIRT are explicitly established.</i>	100
Respond Function	4.8.8 - Establishes management review and approval of the ISIRT on a quarterly basis or to address system/organizational changes or problems encountered during implementation, execution, or testing	IR-8	<i>Suspected security incidents are always reported to the Service Desk.</i>	100
Respond Function	4.8.8 - Establishes management review and approval of the ISIRT on a quarterly basis or to address system/organizational changes or problems encountered during implementation, execution, or testing.	IR-8	<i>The ISIRT manual is reviewed by management and is approved on a bi-annual basis.</i>	75

		Respond Function	4.8.9 - Ensures distribution of updated versions is delivered to ISIRT members.	IR-8	<i>Updated version are appropriately distributed to ISIRT members.</i>	100
		Respond Function	4.8.10 - Protects the ISIRT from unauthorized disclosure and modification.	IR-8	<i>The ISIRT is distributed to authorized members and they are given instructions to keep it secure.</i>	100