Montana University System (MUS)

IT Governance Pillars (see associated IT Governance and Reporting Structure flowchart)

Governance Pillar	Role
MUS IT Council	The MUS IT Council is comprised of the Deputy Commissioner for Budget and Planning, the flagship chief information officers (CIOs), and MUS IT Director. The Council examines potential avenues for shared services and makes recommendations to the Board of Regents (BOR) on ways to align IT, business, and MUS investment strategies.
Flagship Chief Information Officers (CIOs)	Flagship CIOs support the technology needs of their affiliation and the Board of Regents. Affiliated campuses shall coordinate computing purchases and network activities through the flagship CIO. This promotes the sharing of hardware, software, and services and enables the MUS to leverage economies of scale through coordinated procurements and consolidated licensing. Each flagship CIO is responsible for implementing and managing the information security program throughout their affiliation. At least annually, each CIO reports to the IT Council the overall status of and compliance with the information security program and on other matters such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses, and recommendations for changes in the information security program. (16 CFR Part 314)
MUS IT Security Steering Committee	The MUS IT Security Steering Committee helps to identify and communicate IT and security goals and priorities based on flagship CIO initiatives, BOR information technology/security initiatives, and regulatory requirements. This group is facilitated by the MUS IT Director and composed of the flagship CIOs, CISOs, and campus IT leadership from each campus. The Steering Committee helps inform the flagship CIOs and IT Council related to IT and information security needs and risks.
Campus IT Leadership	For all matters related to information technology, IT governance, and information security, IT leadership at affiliated campuses report functionally to the flagship CIO. Campus IT leadership shall coordinate all computing purchases and network activities through the flagship CIO. This promotes the sharing of hardware, software, and services and enables the MUS to leverage economies of scale through coordinated procurements and consolidated licensing. Campus IT leadership shall implement the information security program established by the flagship CIO.
Internal Audit	As the third line of defense, internal audit verifies that the security controls reported are being executed as stated and looks for deficiencies in security that need to be addressed to improve the overall security posture of the organization. Results of audits are reported to the Budget, Administration & Audit Committee regularly. Internal audit reviews other areas related to IT governance as prioritized through risk assessments.
Enterprise Risk Management (ERM)	ERM helps the MUS identify and prioritize the key risks faced by our organization based on risk assessments. Information security risks are inherent to the MUS. To minimize the extent to which information security risks impede the MUS mission effective collaborations among ERM stakeholders and information technology/security subject matters experts is essential. The ERM process also helps to ensure the MUS allocates IT and information security resources appropriately. ERM risk assessments and recommendations for risk management plans are reported to the Budget, Administration, and Audit Committee.