NSCS Information Security Standard 14: Information Systems Security Risk Management

The NSCS Information Security Program shall conduct a periodic review of risks and mitigation strategies. Where possible, an industry standard list of risks in the form of a risk register, such as the Educause IT Governance, Risk, and Compliance (GRC) framework, shall be used. This work shall be integrated with the NSCS Enterprise Risk Management program described in Board Policy 7008.

The review process shall identify the effectiveness of current mitigation strategies and inform the prioritization of risk management activities for the next review cycle.

NSCS Information Technology (IT) risk registers are maintained by the CISO or President's designee at each College, and by the Vice Chancellor for Facilities and Information Technology/SOISO at the System Office. The University of Nebraska performs these functions for the NeSIS and NeBIS enterprise systems. Risk registers at each College and the System Office are shared no less than annually with the President or Chancellor, as applicable, and other administrators as needed for buy-in, acceptance, and funding. The NSCS SOISO and CIO/CISO's will routinely share risks through their on-going meetings and coordination to identify when risks are applicable to a broader stakeholder audience.

Revision History

April/14/2019: Initial submission by PCSS
May/8/2019: Initial review by SOISO/CISOs
July/8/2019: Second review by SOISO/CISOs
July/26/2019: Third review by SOISO
Oct/1/2019: Fourth review by SOISO