New Hampshire Department of Education
Guidance on Acceptable Security Certifications in lieu of the Minimum Standards under RSA 189:66

New Hampshire Department of Education

The purpose of this guidance is to provide acknowledgement and recognition of national or international security assessment and certification standards which meet or exceed the New Hampshire "Minimum Standards for Privacy and Security of Student and Employee Data," as established under RSA 189:66, and may be accepted by Districts in lieu of a specific assessment against the Minimum Standards.

It should further be noted that the list of acceptable security standards may not match up one for one with the Minimum Standards, however all of the national or international security standards listed below either meet or exceed the Minimum Standards in depth and/or breadth, and demonstrate sufficient rigor in applying security and privacy requirements to their respective software application, digital tool, extension or online service.

Therefore, the Department of Education considers that applications or services that can demonstrate successful completion of the following national or international security assessments, authorizations or certifications as meeting or exceeding the Minimum Standards as established under RSA 189:66, and may be accepted by Districts in lieu of a specific assessment against the Minimum Standards:

- NIST SP 800-171 rev 2, Basic and Derived Requirements
- NIST SP 800-53 rev 4 or newer, Low Impact Baseline or higher
- FedRAMP (Federal Risk and Authorization Management Program)
- ISO/IEC 27001:2013
- Center for Internet Security (CIS) Controls, v. 7.1, Implementation Group 1 or higher
- AICPA System and Organization Controls (SOC) 2, Type 2
- Payment Card Industry Data Security Standard (PCI DSS), v3.2.1

Evidence of successful certification based on the preceding security standards could be in the form of a national or international Certification document; an Authorization to Operate (ATO) issued by a state or federal agency, or by a recognized security standards body; or a Preliminary Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB).