# Section A: Risk FACTORS Determination

*Always required except for renewals of Service Contracts & cloud workbooks previously approved by DOIT.*

Agency/division: Department of Education, Division of Learner Support, Bureau of Adult Education

IT Service/Product name: Enter service or product name

Agency contact name, email address, and phone number:

Sarah Wheeler

Sarah.L.Wheeler@doe.nh.gov 603-271-6701

ISO contact name, email address, and phone number:

Bruce Smith

Bruce.V.Smith@doit.nh.gov 603-230-3459

A1: What is the main function of the proposed Cloud or Hosted Service and how will it be used to support one or more business functions? Briefly describe the number of records anticipated and how that number is anticipated to grow over time; the number of users; and the anticipated cost. A completed IT Investment form with the same information may be attached instead, if available.

Click here to enter text.

A2:What data classification level of information will the Cloud or Hosted Service store, process, or transmit? Check all that apply. Consult DOIT Policy NHS0015.10.2011-v.2 "Data Classification Policy" at https://nhstaff.nh.gov/doit/intranet/toolbox/standards/index.php for definitions.

[ ]  Level 1

[ ]  Level 2

[ ]  Level 3 **-> significant risk; also, complete Section B if checked**

[ ]  Level 4 **-> significant risk; also, complete Section B if checked**

A3:Will the proposed Cloud or Hosted Service store, process, or transmit data that must be protected according to the following specialized laws, rules or standards? Check all that apply.

**If any items below are checked, the investment has significant risk; also, complete Section B.**

[ ]  HIPAA (Protected Health Information)

[ ]  CJIS (Criminal Justice Information)

[ ]  IRS Publication 1075 (Federal Tax Information)

[ ]  FERPA (student education records)

[ ]  PCI (Payment Card Information)

[ ]  SSA (Social Security Administration)[ ]  FISMA (Federal Information Security
Modernization Act)

[ ]  MARS-E (Minimum Acceptable Risk
Standards for Exchanges)

[ ]  No checkboxes apply

[ ]  Other, please identify the rule or standard:

Click here to enter text.

A4: Will the Cloud or Hosted Service be the authoritative source for any business-critical information that would be difficult, expensive, or infeasible to recreate? Check one.

[ ]  No (check this box if data in the Service is a copy of another authoritative source; if it could be easily recreated; or if loss or corruption of the data would have no significant consequences)

[ ]  Yes (check this box if loss or corruption of the data would create significant expense, risk, or impact; or it is the system of record) **-> significant risk; also, complete Section B workbook if checked**

A5: Would a sustained interruption of the Cloud or Hosted Service have a significant impact to New Hampshire citizens and to the agency, the State, and partner organizations? Check one.

[ ]  Minor impact. Check this box if agency operations would be able to continue without significant impact to New Hampshire citizens, the agency, the state, or partner organizations.

[ ]  Significant impact. Check this box if an interruption would have anything more than a minor impact**. -> significant risk; also, complete Section B workbook if checked**

A6: Will the Cloud or Hosted Service and all associated data reside entirely within the United States?

[ ]  Yes

[ ]  No **-> significant risk; consult with DOIT before proceeding to complete Section B workbook if checked**

[ ]  Not known **-> significant risk; consult with DOIT before proceeding and complete Section B workbook if checked**

## Agency conclusion:

[ ]  Low Risk: check only if no “significant risk” box above is checked.

[ ]  Significant Risk: check if any one or more “significant risk” boxes above are checked.

### Approving Business Owner signature

First name Last name Title Click here to enter a date

 *Signature*

### Approving Information Technology Lead signature

First name Last name Title Click here to enter a date

 *Signature*

### ISO signature

Bruce Smith Asst Director Click here to enter a date

 *Signature*

# Section B Sub-Section 1: Requirements

*Required when Section A identifies significant risk.*

Agency/division: Department of Education, Division of Learner Support, Bureau of Adult Education

IT Service/Product name: Enter service or product name

Agency contact name, email address, and phone number:

Sarah Wheeler

Sarah.L.Wheeler@doe.nh.gov 603-271-6701

ISO contact name, email address, and phone number:

Bruce Smith

Bruce.V.Smith@doit.nh.gov 603-230-3459

B1-1: What security or privacy controls does the agency expect the cloud or hosted services vendor to have in place to protect state data against unauthorized access ("confidentiality"), loss ("availability"), and corruption ("integrity")? In addition, the vendor must agree to comply with State standards, rules, laws, and policies, as they are updated from time to time. The current state standards are available at: https://nhstaff.nh.gov/doit/intranet/toolbox/standards/index.php

Click here to enter text.

B1-2: What are your business requirements for availability? This answer should represent the tolerance of supported business processes to planned and unplanned outages. Note acceptable downtime, planned and unplanned, during regular business hours and off hours.

Click here to enter text.

B1-3: Document minimum requirements that the vendor must meet to comply with agency or state incident management requirements, to include the Statewide Cyber Disruption Plan. Requests to see the Statewide Cyber Disruption Plan should be sent to NH-CIC@doit.nh.gov

Click here to enter text.

B1-4: Document agency requirements to maintain ownership of data to include retention, destruction requirements as needed and restrict usage by the vendor. Be sure to address metadata and derived data.

Click here to enter text.

B1-5: How will the agency document and verify (audit) that the vendor has appropriate controls in place to deliver on the confidentiality, availability, and integrity commitments documented in this worksheet and the Service Contract? Vendors must typically agree to carry out regular third-party audits with specified scope and standards and must agree to promptly provide such audit results to the agency.

Click here to enter text.

### Approving Business Owner signature

First name Last name Title Click here to enter a date

 *Signature*

### Approving Information Technology Lead signature

First name Last name Title Click here to enter a date

 *Signature*

### ISO signature

Bruce Smith Asst Director Click here to enter a date

 *Signature*

# Section B Sub-Section 2: Contract and related planning

*Required when Section A identifies significant risk.*

Agency/division: Department of Education, Division of Learner Support, Bureau of Adult Education

IT Service/Product name: Enter service or product name

Agency contact name, email address, and phone number:

Sarah Wheeler

Sarah.L.Wheeler@doe.nh.gov 603-271-6701

ISO contact name, email address, and phone number:

Bruce Smith

Bruce.V.Smith@doit.nh.gov 603-230-3459

 B2-1: Document how the Contract ensures appropriate protection of the data against unauthorized access ("confidentiality"), loss ("availability"), and corruption ("integrity").

Click here to enter text.

B2-2: Document how the Contract requires the vendor to maintain disaster recovery systems and processes sufficient to protect agency interests.

Click here to enter text.

B2-3: Does the agency have strategies for both planned and unplanned exit from the Cloud or Hosted Service? Briefly describe them. Consider plans for data transfer at exit or termination. Document how the Contract supports the agency's exit strategy, including how it codifies vendor and agency responsibilities during exit planning and during planned or unplanned exit.

Click here to enter text.

B2-4: Document how the Contract binds the vendor to deliver required service levels.

Click here to enter text.

B2-5: Describe how the IT incident, security incident and change management processes and the responsibilities of each party are spelled out in the Contract.

Click here to enter text.

B2-6: Document how the Contract defines data ownership and rights for the vendor and the agency. Be sure to address metadata.

Click here to enter text.

B2-7: Document how the Contract captures appropriate data retention and destruction commitments from the vendor, including (as necessary) a commitment to certify data destruction meeting NIST SP 800-88 standards.

Click here to enter text.

B2-8: Document how the Contract requires the vendor to perform, cause to be performed by a third party, and/or cooperate with audits. Document what audit results must be provided to the agency. Note what standards of audits apply (for example, SOC 2 Type 2), how frequently audits must be performed, whether the state will obtain complete findings, and how promptly results must be shared with the state.

Click here to enter text.

### Approving Business Owner signature

First name Last name Title Click here to enter a date

 *Signature*

### Approving Information Technology Lead signature

First name Last name Title Click here to enter a date

 *Signature*

### ISO signature

Bruce Smith Asst Director Click here to enter a date

 *Signature*