



Securing Your Ecosystem

LTI Audit Checklist for Institutions



Purpose

Before you can strengthen the security of your edtech ecosystem, you need to know what's connected to it. While your LMS may support the most current version of Learning Tools Interoperability (LTI)[®] (LTI 1.3), some learning tools, departmental applications, or homegrown solutions may still rely on older integrations that no longer meet current security best practices.

This checklist helps you identify where LTI is used, determine which connections should be upgraded, and prioritize next steps for a more secure, interoperable learning environment.

1. Inventory All External Learning Tools

Identify every tool or app connected to your LMS:

ITEM	CHECK
LMS course placements reviewed	☐
App/tool admin area reviewed	☐
Vendor list reviewed	☐
Procurement/contracts reviewed	☐
Faculty-submitted tools identified	☐
Department-specific tools identified	☐
Vendor list reviewed	☐
Custom or homegrown tools identified	☐

Click the hyperlink to find a spreadsheet version of the [LTI Audit Inventory](#) to track each tool or app.

For each tool, record:

FIELD	NOTES
Tool name	
Vendor/contact	
LMS/platform used	
LTI version currently used	LTI 1.0 / 1.1 / 1.2 / 1.3 / unknown
Placement type	Course nav, assignment, module link, editor button, etc.
Courses using tool	
Number of active users	
Data exchanged	Name, email, role, course, grades, roster, etc.
Gradebook integration?	Yes / No
Roster sync?	Yes / No
Content selection?	Yes / No
Accessibility reviewed?	Yes / No
Security/privacy reviewed?	Yes / No
Contract renewal date	
Number of active users	
Institutional owner	

2. Identify LTI 1.3 Implementations

Label each tool:

STATUS	DEFINITION
Certified	Achieved 1EdTech certification for LTI 1.3 Core and related feature services, if required
Compliant	Uses LTI 1.3 and related services
Partially	Uses LTI 1.3 launch but lacks needed LTI feature services
Legacy	Uses LTI 1.0, 1.1, 1.2, custom API, or SSO workaround
Unknown	LTI version or configuration cannot be confirmed
Not needed	No longer actively used or has low-value use case

Products that earn 1EdTech certification have been tested for functionality and security and are listed on 1edtechcert.org.



3. Determine Application Risk Level

Using the core information collected for each application, assess its risk level using the criteria below:

RISK	CRITERIA	RECOMMENDED ACTION
Low	Tool fully supports LTI 1.3 and any related services (Deep Linking, Names and Role Provisioning Services, Assignment and Grade Services) required by the institution. Vendor actively maintains integration and has current 1EdTech certification.	No action needed beyond annual review.
Medium	Tool has implemented LTI 1.3 but required feature services are missing or the vendor has announced migration plans but legacy integrations remain in use.	Coordinate migration with vendor and defined timelines.
High	Tool relies on LTI 1.0, 1.1, 1.2, custom authentication, shared secrets, or proprietary integrations. Vendor has no published migration timeline or no current 1EdTech certification for LTI 1.3.	Prioritize migration or replacement. Review contract renewal and procurement implications.

4. Prioritize Which Tools Need Action

Assign priority:

PRIORITY	CRITERIA
High	Handles grades, PII, large enrollments, required coursework, or high institutional risk
Medium	Used regularly but limited data exchange or lower enrollment
Low	Small pilot, optional use, no sensitive data, or near retirement



5. Vendor Readiness Questions

Send technology providers these questions:

- Do you currently support LTI 1.3?
- Which LTI 1.3 services do you support?
 - Deep Linking
 - Assignment and Grade Services
 - Names and Role Provisioning Services
- Are you 1EdTech certified for LTI 1.3 and related feature services?
- Do all of your integrations use LTI 1.3?
If not, what tools use other integrations?
- Do you have a process to migrate us from your LTI 1.1 version of your app to the LTI 1.3 version of your app?
- Will anything in our existing courses or assignments be affected by the migration?
- What instructions or resources for migration do you provide for our LMS? Can we test everything before going live?
- What is a realistic timeline for completing the migration?
- Will we lose any functionality or need to change any workflows during the migration?
- What support will be available before, during, and after the migration?



6. Risk Review for Legacy Tools

Use this section for any tool not yet on LTI 1.3:

RISK AREA	REVIEW QUESTION	STATUS
Privacy	Is unnecessary user/course data shared?	☐
Support	Is the vendor still supporting this integration?	☐
Compliance	Does the tool meet institutional policy?	☐
Continuity	Would disabling the tool disrupt active courses?	☐

7. Determine Migration Decision

For each tool, choose one path:

DECISION	WHEN TO USE
Migrate	Vendor supports LTI 1.3 and tool remains needed
Replace	Vendor does not support LTI 1.3 or lacks required services
Retire	Tool has low/no usage or duplicate functionality
Exception	Tool is temporarily allowed with documented risk and end/migration date

8. Step-by-Step Migration Process

Once you've identified which tools are still using outdated integrations, the next step is creating a plan to migrate them to LTI 1.3. This step-by-step guide will help you prioritize upgrades, work with your edtech providers, and transition to modern, secure interoperability with confidence.

Step 1: CONFIRM CURRENT STATE

- Confirm current LTI version
- Document all placements and courses using the tool
- Identify data passed to/from the tool
- Confirm gradebook, roster, and content selection needs

Step 2: CONFIRM TARGET STATE

- Confirm LTI 1.3 support
- Confirm needed LTI 1.3 services and conformance evidence (Ideally via 1EdTech Certification)
- Confirm institutional security/privacy requirements
- Confirm accessibility documentation
- Confirm all needed functionality exists in the new version.
- Confirm documentation on how to utilize the tool in the new version (if process changes after migration)

Step 3: CONFIGURE AND VALIDATE THE LTI 1.3 INTERGRATION IN A TEST ENVIROMENT BEFORE DEPLOYING TO PRODUCTION.

- **Recommended Practice:**
If your institution has access to a test or staging environment, complete initial configuration and validation there before enabling the integration in production. If a test environment is not available, work with your LMS and tool provider to identify alternative testing options or conduct testing during a planned maintenance window to minimize disruption to instructors and students.
- Register tool in LMS test environment
- Enable required placements
- Enable required services
- Limit data sharing to necessary fields

Step 4: CONFIRM THAT THE UPDATES WORK AS EXPECTED

- Instructor launch works
- Student launch works
- Correct roles are passed
- Course/context information is correct
- Deep linking works, if required
- Roster access works, if required
- Grade passback works, if required
- Existing content links are tested
- Mobile/app behavior is tested
- Accessibility and privacy checks are complete

Step 5: PARTNER WITH TOOL PROVIDER. PLAN ROLLOUT.

- Identify pilot courses
- Notify faculty/admin users
- Provide migration instructions
- Define support escalation path
- Set cutover date
- Set legacy tool disable date

Step 6: MIGRATE PRODUCTION

- Register production LTI 1.3 tool
- Validate launch and services
- Migrate or recreate links (Depending on your processes, educators may require training.)
- Confirm gradebook behavior
- Monitor first-week support issues
- Disable legacy integration after validation

Step 7: CLOSE AUDIT ITEM

- Update institutional tool inventory
- Record final LTI status
- Store configuration documentation
- Store vendor confirmation/certification evidence
- Schedule annual review

9. Final Audit Summary

Record your migration status:

CATEGORY	COUNT
Total tools reviewed	
LTI 1.3 certified	
LTI 1.3 compliant	
LTI 1.3 partial	
Legacy/non-LTI 1.3	
Unknown status	
To migrate	
To replace	
To retire	
Exceptions approved	

10. Success Target

TARGET STATE

100% of institutionally supported tools using certified LTI 1.3, with related services enabled where required.

EXCEPTION POLICY

Any remaining non-LTI 1.3 integration must have:

- Documented business justification
- Approved risk acceptance
- Target retirement date
- Annual review requirement

11. Recommended Governance Cadence

Establish an ongoing schedule:

FREQUENCY	ACTIVITY
Each Term	Review new tool requests
Bi-Annually	Audit active LTI tools
Annually	Review all vendor LTI status and certification evidence
Before Launch	Complete security, privacy, accessibility, and LMS testing



Make technology audits a regular part of your IT governance.

Periodically reviewing your integrations helps uncover outdated connections, strengthen security, and ensure your edtech ecosystem continues to support current interoperability standards.

Together is the New Standard

Go to 1EdTech.org for more info on Learning Tools Interoperability.

