

The easier way to avoid the financial and reputational costs of GLBA non-compliance

Isora GRC from SaltyCloud is the ideal automated assessment solution for Title IV Schools seeking a simple, cost-effective approach to achieving GLBA and NIST 800-171 compliance.

Challenge

With cyber threats on the rise, Title IV Schools (EDUs) face serious financial consequences if they can't prove they are meeting their legal obligations to protect student financial data.

The U.S. Department of Education Financial Student Aid (FSA) designates data used to administer federal student aid programs as controlled unclassified information (CUI)¹. It requires EDUs to safeguard it under the requirements of the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule.

Among the requirements, EDUs must adopt a security framework like NIST 800-171, conduct a risk assessment against that framework, and document safeguards for identified risks.

The FSA has warned EDUs in violation of the GLBA Safeguards Rule that they face losing access to the FSA's information systems (effectively halting their ability to service students), and having adverse audit findings referred to the Federal Trade Commission (FTC), which has the power to fine offending organizations and even individuals in charge of safeguarding CUI (e.g., CISOs, Security Analysts, Compliance Managers, etc.)².

The potential serious financial consequences of not meeting these requirements—not to mention the reputational impact an Institution could suffer—means EDUs must have a reliable process in place that demonstrates they are complying with the GLBA.

Given the number of staff across the EDU whose input is required and the need for an evidentiary audit trail, a spreadsheet-based approach to managing risk and compliance is no longer adequate or efficient. But, at the same time, most EDUs don't have the resources to deploy expensive and complex GRC solutions.

Business challenges

- > Keeping up with regulatory requirements including GLBA and FSA mandates
- > Avoiding audit findings and potential penalties
- > Balancing limited budgets, resources, and FTEs
- > Maintaining information security at scale

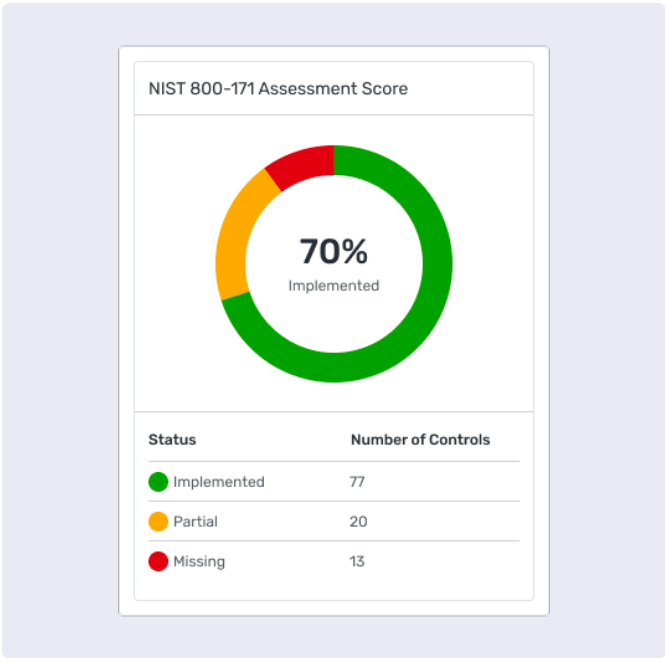
Workflow challenges

- > Conducting a cybersecurity risk assessment every year
- > Documenting and tracking safeguards for identified risks
- > Managing compliance data across multiple covered units
- > Creating audit-ready evidentiary reports

Solution

Isora GRC from SaltyCloud is an assessment platform designed specifically to meet the governance, risk, and compliance (GRC) needs of EDUs.

The solution makes compliance requirements like the GLBA Safeguards Rule easier by automating and centralizing your assessment workflow—helping your EDU align with a security framework, manage risk over time, and demonstrate compliance all on a streamlined platform.



Outcomes & benefits

- ✓ Ace your audit and avoid penalties with evidentiary and audit-ready compliance reports.
- ✓ Reduce noise and conserve valuable resources with an automated assessment workflow.
- ✓ Justify budgets and information security initiatives with confidence using powerful risk insights.
- ✓ Improve your organization’s security posture with continuous risk monitoring.

Key features & capabilities

Automated assessments

Create, customize, and launch risk and compliance assessments with our automated questionnaire engine.

Pre-loaded frameworks

Use our library of information security frameworks like NIST 800-171, NIST CSF, and more.

Intuitive reporting

Identify organizational risks using executive dashboards, in-depth risk reports, and comparative reports.

Continuous monitoring

Launch reassessments on a yearly basis and continuously monitor and track improvements.

Hassle-free compliance

Establish a system of record and export audit-ready reports to demonstrate regulatory compliance.

Easy deployability

Deploy Isora GRC across the organization without the need for dedicated teams.

On-demand training

Get your organization up and running with comprehensive online training materials and personalized training.

U.S. Department of Education, Office of Inspector General GLBA audit procedures

As part of their annual federal compliance audits submitted to the U.S. Department of Education (Department) Office of Inspector General, EDUs must prove they comply with the GLBA Safeguards Rule and its requirements. To determine compliance, the Department requires auditors to perform several procedures³.

Section	Procedure	Recommendation
C.8.12.b.	Verify that the institution has performed a risk assessment that addresses the three required areas noted in §314.4(b) of the GLBA Safeguards Rule: 1. Employee training and management; 2. Information systems, including network and software design, as well as information processing, storage, transmission and disposal; 3. Detecting, preventing and responding to attacks, intrusions, or other systems failures.	<ul style="list-style-type: none">• Use Isora GRC to launch a risk assessment using security frameworks such as NIST 800-171 or NIST CSF (pre-loaded in the solution).• Create a custom questionnaire that covers the required areas noted in §314.4(b).• Target your assessment to departments that handle FSA data (e.g., financial aid office, registrars office, bookstore, etc.)• Generate and export an audit-ready report that shows department scores and identified risks.
C.8.12.c.	Under §314.4.(c) of the Safeguards Rule, verify that the EDU has documented a safeguard for each risk identified above.	<ul style="list-style-type: none">• Use Isora GRC to have respondents document safeguards as they go through their risk assessment questionnaire.• Generate and export an audit-ready report that includes documented safeguards for identified risks.

For a comprehensive guide to meeting GLBA requirements download our eBook, [Ace your GLBA Audit, The Step-by-Step Guidebook \(2021 Edition\)](#)

Ready to ace your audit?

Get a guided tour of Isora GRC from SaltyCloud and ask us about features, implementation, and pricing.

GET A DEMO

CONTACT US

Berkeley
UNIVERSITY OF CALIFORNIA



VT VIRGINIA
TECH.

TDI Texas Department
of Insurance

"Isora GRC is helping our university system align itself with the NIST Cybersecurity Framework (CSF), identify and resolve GLBA compliance gaps, but most importantly, approach our GLBA audit with confidence while freeing our team's valuable hours."

Information Security Manager

Large Midwestern University System

1 Protecting Student Information – Compliance with CUI and GLBA, December 18, 2020, <https://fsapartners.ed.gov/fsa-print/publication/49974>

2 Enforcement of Cybersecurity Requirements under the Gramm-Leach-Bliley Act, February 28, 2020, <https://fsapartners.ed.gov/fsa-print/publication/29325>

3 Dear CPA Letter CPA-19-01, October 30, 2019, <https://www2.ed.gov/about/offices/list/oig/nonfed/cpa1901.pdf>

