

Cyber Risk & Compliance Built for Banking

Quantitative risk assessments, automated evidence, and unified oversight for banks and credit unions.

THE CHALLENGE

Spreadsheet Risk Assessments, Disconnected Workflows, and No Way to Prove It

Most financial institutions still run risk assessments in spreadsheets with inconsistent scoring that is difficult to defend. Control evidence lives in scattered folders and shared drives. Risk, compliance, and governance workflows operate in silos, leaving critical exposures unaddressed and making it nearly impossible to show a connected picture of institutional risk posture.

Generic GRC platforms lack alignment to FFIEC, GLBA, and NIST expectations. They cannot connect risk scores to evidence, controls to frameworks, or cyber posture to business outcomes. The result: lean teams buried in manual prep, limited board visibility, and risk postures that fall apart under examiner scrutiny.

THE SOLUTION

Prove Risk Oversight with Receipts, Not Promises

DefenseStorm Cyber Risk & Compliance unifies risk assessments, control monitoring, and governance workflows into a single, banking-specific platform. Run quantitative GLBA and asset-based assessments with defensible scoring. Maintain centralized risk and control registers. Attach system-generated evidence to every control so scores are always backed by proof, not assumptions.

The result: fewer vendors, less manual effort, and a defensible risk posture that holds up with examiners and boards alike.

KEY CAPABILITIES

What You Get

A purpose-built platform that consolidates overlapping risk, compliance, and governance workflows into one view, replacing tool sprawl and disconnected processes with board-ready dashboards and examiner-trusted evidence.



Quantitative Risk Assessments

Run GLBA and asset-based risk assessments with defensible, evidence-backed scoring tailored to your institution's risk tolerance. Centralized risk and control registers standardize methodology across every assessment.



Automated Evidence Collection

Connect controls to system-generated evidence so scores are always backed by proof, not assumptions. Automated artifact generation reduces manual evidence collection by 20+ hours per month.



Framework Mapping & Governance Workflows

Align risks and controls to FFIEC, GLBA, NIST, InTReX, and ISE automatically. Validate controls, assign ownership, and track changes with full version control and audit trails.



Executive Dashboards & Board Reporting

Real-time risk posture, KPIs/KRIs, maturity trends, and remediation priorities delivered in language leadership can act on, in formats boards and examiners expect.

Outcomes That Move the Needle



Defensible Risk Assessments

Run GLBA and asset-based assessments with quantitative, evidence-backed scoring. Centralized risk and control registers standardize methodology so every score is consistent, repeatable, and exam-ready.

Key outcome: Risk scores backed by proof, not assumptions. Every finding holds up under scrutiny.



Automated Evidence, Zero Manual Prep

System-generated evidence attaches directly to controls so artifact collection happens continuously, not before exams. Automated mapping cuts manual evidence prep by 20+ hours per month.

Key outcome: Exam prep becomes an ongoing process. Teams focus on oversight, not artifact assembly.



Unified Risk & Governance Oversight

Consolidate risk assessments, control monitoring, and governance workflows into one platform. Connect cyber risk, control effectiveness, and compliance posture into a single picture of institutional risk.

Key outcome: Fewer vendors, fewer gaps. One connected view of risk posture and control effectiveness.



Board-Ready Visibility

Real-time dashboards translate cyber and governance posture into clear business terms. KPIs, KRIs, maturity trends, and remediation priorities delivered in the language leadership can act on.

Key outcome: Leadership sees risk clearly. Boards get evidence they trust.

Risk Oversight with Receipts, Not Promises

DefenseStorm Cyber Risk & Compliance replaces scattered tools and manual processes with a unified platform where every risk score, control status, and governance workflow is backed by system-generated evidence. Integrated with DefenseStorm MDR and Governance & Monitoring for a complete picture of institutional risk posture. Low-lift onboarding with 160+ parsers and 1,900+ integrations. Case management and audit trails deliver defensible, exportable records for investigations and remediation.

Why DefenseStorm



Built for Banking

Purpose-built for banks and credit unions, not a generic GRC tool adapted for financial services. Every workflow, framework, and report reflects FI oversight expectations.



Unified Risk and Governance View

Connect cyber risk, control effectiveness, governance workflows, and compliance posture into a single platform. Fewer vendors, fewer gaps, one connected picture.



Evidence-Based Assurance

Automated mapping to FFIEC, GLBA, and NIST translates to board-ready artifacts and examiner-trusted outputs. Risk scores are backed by proof, not promises.



Operational Efficiency

Automated artifact generation and continuous monitoring reduce manual effort by 20+ hours per month, freeing lean teams to focus on risk reduction rather than evidence assembly.



Trusted by Peers, Recognized by Examiners

Proven across 200+ banks and credit unions. Customers consistently cite DefenseStorm's banking knowledge, responsiveness, and examiner credibility as key differentiators.

By the Numbers

138+

Exam-ready artifacts generated per month

20+ hrs

Saved monthly on manual evidence collection

91%

Detection triggers mapped to regulatory controls

38%

Reduction in residual risk within 12 months

47%

Fewer critical control failures within 12 months

2.4

Avg. framework maturity improvement over 3 quarters

100%

GLBA and FFIEC alignment with real-time dashboards

160+

Custom parsers for broad telemetry coverage

200+

Banks and credit unions protected

Risk oversight backed by proof. **Compliance posture built to last.**

Ready to replace spreadsheets with examiner-ready oversight? See how DefenseStorm Cyber Risk & Compliance works for institutions like yours.

470-519-0020

info@defensestorm.com