Contents

RFP: CSH IT Systems Cybersecurity Audit & Systems Integration Review

Executive Summary

Objective

Corporation for Supportive Housing (CSH) seeks proposals from qualified independent third-party firms to:

1. **Validate cybersecurity posture** across the enterprise environment
2. **Assess and rationalize system integrations** and systems of record

Outcome We Need

- Independent, evidence-based assessment of cybersecurity posture and key control gaps
- Clear current-state view of systems of record, integrations, and data flows
- Prioritized recommendations to strengthen security, integration maturity, and data governance
- Practical roadmap to support near-term action and longer-term improvement

Critical Principle

CSH seeks to preserve independence and objectivity between assessment and implementation. Any potential implementation role by the selected vendor or an affiliated entity must be disclosed, reviewed, and approved by CSH with appropriate conflict mitigation safeguards.

Organizational Context

CSH is a national non-profit that functions both as a technical assistance provider in the supportive housing field and as a Community Development Financial Institution (CDFI) that provides loan products to supportive and affordable housing developments across the country. CSH operates a multi-system environment across HR, finance, loan administration, CRM, training, communications, and analytics (42 systems identified to date in the CSH Software Systems inventory). Listing of systems will be available upon execution of CSH RFP NDA.

Examples include:

- HRIS (e.g., Paycom)
- Contract and signature tools (e.g., DocuSign)
- Financial and operational platforms (e.g., NetSuite)
- Loan management (TEA)
- Collaboration tools (Microsoft ecosystem, Zoom)
- Data and reporting platforms

This environment requires improvement:

- Visibility into current security posture
- Clarity on systems of record and integrations
- Stronger data integrity and accountability practices

RFP: CSH IT Systems Cybersecurity Audit & Systems Integration Review

Scope of Work

Phase 1: Cybersecurity & IT Systems Audit

Objective

Assess CSH's enterprise IT network, systems, and data environment to identify material cybersecurity risks, control gaps, and remediation priorities in alignment with recognized industry practices.

Required Activities

Enterprise Security Assessment

- Identity & access management (Entra/Azure AD environment)
- MFA and authentication controls
- Role-based access (RBAC) review
- Privileged access management

Infrastructure & Endpoint Security

- Device management (e.g., Intune)
- Endpoint protection (e.g., Sophos)
- Patch management and vulnerability exposure

Unmanaged Device & BYOD Risk Assessment

The vendor must assess risks associated with access to CSH systems from unmanaged or non-compliant devices, including personal (BYOD) environments.

This assessment must include:

- Identification of current access pathways from unmanaged devices
- Evaluation of risks related to remote work, personal devices, and external network access
- Alignment with conditional access and device compliance policies
- Identification of potential exposure pathways for malware, credential compromise, and data loss

The vendor must recommend controls to reduce or eliminate access risk from unmanaged devices, where appropriate.

Technical Enforcement of Integration Restrictions

The vendor must evaluate whether technical controls are in place to enforce integration and software restrictions, including:

- Role-based access controls (RBAC) limit who can create or authorize integrations
- Conditional access or administrative controls restricting integration permissions
- Restrictions on application consent and third-party app authorization
- Device and system controls limiting software installation

The vendor must identify where reliance is placed on policy alone rather than enforceable system controls.

Network & Cloud Security

- Configuration and exposure review

- Data loss prevention (DLP)
- Conditional access policies

Application Security

- Review security posture across key business systems (42+ systems)
- Evaluation:
    - Authentication methods
    - Data storage risks
    - Vendor security alignment

Unauthorized Software, API, and Integration Control Assessment

The vendor must assess controls that prevent unauthorized addition, configuration, or use of:

- APIs and API connections
- EDI integrations or external data exchange mechanisms
- Third-party software applications (installed or cloud-based)
- Integration tools (e.g., connectors, middleware, automation platforms)

This assessment must evaluate whether CSH has effective controls to:

- Restrict the ability of staff to independently create or enable integrations
- Require formal approval and validation prior to any system-to-system connection
- Enforce use of authorized systems and integration pathways only
- Detect unauthorized or unapproved integrations or software usage

The vendor must identify any gaps where staff could introduce integrations or tools outside of defined governance processes.

Third-Party & Vendor Risk Assessment (Expanded Requirement)

In addition to evaluating application-level security, the vendor must assess risks associated with third-party systems and dependencies.

This must include:

- Review of vendor security controls and alignment with CSH requirements
- Assessment of vendor breach notification capabilities and contractual alignment
- Identification of single points of failure across critical vendor dependencies
- Evaluation of vendor continuity and disaster recovery capabilities

The vendor must identify where vendor dependencies introduce elevated risk to operations, data security, or continuity.

Data Security & Privacy

- Data classification and governance
- Encryption practices
- Backup and recovery processes

Business Continuity & Recoverability Assessment

The vendor must evaluate the organization's ability to maintain and restore operations in alignment with CSH's Business Continuity Plan.

This assessment must include:

- Validation of backup and recovery capabilities across critical systems
- Evaluation of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), where defined
- Identification of gaps between documented recovery procedures and actual system capabilities
- Assessment of dependencies that may impact recovery (e.g., vendor reliance, integration dependencies)

The vendor must identify risks where recovery may not be achievable within expected timeframes and recommend mitigation actions.

Monitoring & Incident Response

- Logging and audit trail review
- Incident detection and response readiness
- Integration of threat intelligence tools (e.g., Hacknotice)

Automated Detection & Notification Requirement

The vendor must evaluate the existence and effectiveness of automated monitoring and alerting mechanisms related to unauthorized system changes.

This includes:

- Detection of new API connections, external integrations, or third-party application authorizations
- Monitoring for installation or use of unapproved software or tools
- Alerts triggered by changes to system configurations, permissions, or data flows
- Integration with centralized logging and security monitoring systems

The vendor must assess whether automated alerts are:

- Generated in real time or near real time
- Routed to appropriate owners (IT, Security, or designated roles)
- Tracked and resolved through formal incident or escalation workflows

The vendor must identify gaps where unauthorized activity could occur without detection or timely notification.

Deliverables

- Security Risk Assessment Report (prioritized by severity)
- Control Maturity Rating (e.g., NIST or CIS mapped)
- Gap Analysis + Remediation Plan

ERM Risk Alignment Requirement

All identified risks must be mapped to CSH's Enterprise Risk Management (ERM) categories, including but not limited to:

- Governance and policy enforcement
- Cybersecurity control effectiveness
- Vendor and third-party risk
- Data protection and privacy
- Workforce and operating environment risks

For each identified risk, the vendor must:

- Assign a recommended **business owner (role-based, not individual)** (e.g., IT, Finance, CPAO, Legal/Compliance)
- Define **measurable indicators** that can be used for ongoing ERM monitoring and reporting
- Identify whether the risk is **new, existing, or partially mitigated**

Outputs must be structured to support direct integration into CSH's ERM reporting process.

- Executive Summary for Board/Leadership
- Immediate Risk Alerts (within 48 hours of discovery)

Phase 2: Systems Integration & Data Integrity Review

Objective

Validate **systems of record**, map integrations, and establish **reconciliation controls**.

Required Activities

A. Systems of Record Validation

- Identify system of record for:
    - HR data
    - Financial data
    - Loan administration data
    - CRM/client data
    - Learning/training data
- Identify duplication risks or competing systems

Systems Governance & Ownership Requirement

CSH currently has a data governance lead and cross-agency committee that oversees software adoption and technology policies. The vendor must recommend how the current governance model can be adapted in a more mature data environment. Beyond identification of systems of record, the vendor must recommend a governance model to ensure sustained data integrity and accountability.

This must include:

- Recommended ownership model for each system (role-based)
- Definition of data ownership and accountability across systems
- Governance processes for each system and across systems to maintain system-of-record integrity over time
- Recommended review cadence to validate data alignment and reconciliation processes

The vendor must identify risks where governance gaps may lead to data inconsistency or control failure.

B. Integration Mapping

- Document all integrations:
    - API connections
    - Manual processes (critical risk area)

    - Third-party connectors (e.g., Zapier)
- Create a **current-state architecture diagram**

Integration Inventory & Traceability Requirement

The vendor must validate whether CSH maintains a complete and current inventory of:

- All API connections
- System integrations
- Third-party data exchange mechanisms
- Automation or workflow tools impacting data movement

This must include:

- Ownership (role-based) for each integration
- Business purpose and data exchanged
- Direction of data flow
- Last validation or review date

The vendor must identify gaps where integrations exist without clear ownership, documentation, or auditability.

C. Data Flow & Dependency Mapping

- End-to-end data lifecycle:
    - Entry → Transformation → Storage → Reporting
- Identify points of:
    - Data loss
    - Latency
    - Manual intervention
    - End of life
        - data retention

D. Reconciliation & Data Integrity Controls

Define recommended reconciliation and data integrity controls, including:

- Automated reconciliation checks between systems
- Exception reporting processes
- Audit logs and traceability

E. System Rationalization Recommendations

- Identify:
    - Redundant systems
    - Underutilized tools
    - High-risk integrations
- Recommend:
    - Consolidation opportunities
    - Integration strategy (API-first, middleware, etc.)

Deliverables

- Systems Architecture Map (visual + narrative) including documenting the current and recommended structure.
- Systems of Record Matrix
- Integration Inventory
- Data Flow Diagrams
- Reconciliation Control Framework
- System Rationalization Recommendations
- Recommendation for long term critical data storage.
- Implementation Readiness Deliverable including a sequenced roadmap of recommended actions, identification of internal owners (roles, not individuals), required capabilities, dependencies between actions, a required executive briefing session, and a manager-level translation session focused on what needs to change in behavior.
- Roadmap for integration of systems.

Ongoing Monitoring & Sustainability Requirement

The vendor must provide recommendations for sustaining improvements beyond the initial assessment.

This must include:

- Recommended monitoring mechanisms for key risk and control areas
- Suggested metrics or indicators for ongoing tracking (e.g., access compliance, system reconciliation, incident trends)
- Identification of reporting structures to support leadership and ERM oversight
- Opportunities for automation to reduce reliance on manual controls

Outputs should enable CSH to transition from point-in-time assessment to ongoing risk management and governance.

Cross-Phase Requirement: Actionable Recommendations

The selected vendor must provide clear, prioritized, environment-specific recommendations that translate assessment findings into practical next steps across both Phase 1 and Phase 2.

Actionable Recommendations Requirement

Recommendations must clearly define:

- What should change
- Why the change is needed (risk, efficiency, or control gap)
- Expected benefits, including risk reduction, improved data integrity, increased operational efficiency, and enhanced user experience
- Level of effort and complexity
- Dependencies or prerequisites

Recommendations must be:

- Prioritized as High / Medium / Low
- Structured into immediate actions (0–90 days), short-term improvements (3–9 months), and long-term strategic changes (9–24 months)

Behavior Change & Adoption Requirement

In addition to technical recommendations, all findings must translate into clear behavior and workflow changes required for successful adoption.

For each major recommendation, the vendor must define:

- What **staff, managers, and system owners must do differently**
- Where current workflows or behaviors introduce risk
- Common workarounds or points of breakdown
- Risks associated with non-adoption

The vendor must also provide guidance on:

- How new behaviors should be reinforced (e.g., policy, system controls, training, monitoring)
- Where accountability should sit across business functions

Recommendations that do not address behavior and adoption will be considered incomplete.

Integration Governance Enforcement Requirement

The vendor must assess and provide recommendations for enforcing centralized governance overall system integrations and software adoption.

This includes evaluating whether:

- Staff are prohibited from independently enabling APIs, integrations, or software connections
- All integrations are reviewed and approved through a formal governance process
- A centralized inventory of integrations and connections is maintained and updated
- System permissions limit the ability to create or modify integrations to authorized roles only

The vendor must identify where governance controls are insufficient or inconsistently enforced and recommend enforcement mechanisms.

Maturity Model Requirement

Vendors must assess and score CSH's current-state maturity using a clear and defined maturity model. At a minimum, the proposal and final deliverables must include maturity scoring across security maturity, integration maturity, and data governance maturity. Vendors must explain the basis for the scoring approach and describe what is required to advance to the next maturity level in each area.

Early-Win Recommendation Requirement

Vendors must identify early-win recommendations, including a "Top 5 actions within 30 days" list, to enable CSH to begin reducing risk and improving operations immediately while longer-term work is being planned.

Important Constraint

Vendors must avoid generic recommendations and instead align recommendations specifically to CSH's environment and system landscape.

Conflict of Interest Requirement

Vendors must:

- Disclose whether they or any affiliated entity may seek to provide implementation services related to findings or recommendations from this engagement. CSH's preference is to preserve independence between assessment and implementation. Any proposed implementation role by the vendor or an affiliate must be separately disclosed, reviewed, and approved by CSH, and must include appropriate safeguards, such as separate teams, no involvement by assessment personnel in implementation sales decisions, and conflict mitigation measures acceptable to CSH.
- Disclose any partnerships with vendors in the current technology stack. Full list available upon execution of CSH NDA for interested applicants.
- Provide mitigation strategy for any perceived conflicts.
- Disclose any partnerships with vendors in the current technology stack. Full list available upon execution of CSH NDA for interested applicants. **NDA will be sent via Docusign upon request**.
- Provide mitigation strategy for any perceived conflicts

Vendor Qualifications

Vendors should demonstrate:

- Experience in nonprofit or mission-driven organizations
- Expertise in:
    - Microsoft 365 / Azure ecosystems
    - Cybersecurity frameworks (NIST, CIS, ISO 27001)
    - Systems integration and enterprise architecture

Required Capabilities

- Independent security auditing
- Systems architecture modeling
- Data governance expertise

Proposal Requirements

Proposals must include the following components:

Approach & Methodology

- Audit framework
- Integration review approach
- Tools and techniques used

Work Plan

- Phases, milestones, deliverables, and sequencing
- Stakeholder engagement plan aligned to the requirements below

Internal Stakeholder Engagement Requirements

The vendor must incorporate structured engagement with key CSH personnel to ensure findings reflect operational reality and support adoption.

Required Participants May Include

- IT leadership and cybersecurity leads
- System owners (e.g., NetSuite administrator)
- Business system owners (HR, Finance, CRM, Training, etc.)
- End-user representatives
- Administrative and operations staff

Note: CSH maintains internal system expertise, including a dedicated NetSuite lead and internal user support staff.

Vendor Must Propose an Interview Strategy That Includes

1. **Interview Approach**
   Number and type of interviews; role-based grouping (e.g., system owners vs. end users); and interview format (individual vs. group sessions)
2. **Key Topics Covered**
   System usage and dependencies; integration pain points; data accuracy and reconciliation challenges; workarounds and manual processes; and security and access concerns
3. **Documentation Method**
   How findings will be captured and validated, and how discrepancies across stakeholder perspectives will be resolved
4. **Time Expectations for Staff**
   Clear estimate of staff time required per participant and in total

Output Requirement

The vendor must translate interview findings into identified risks or inefficiencies, integration or system gaps, and behavior or workflow changes required to support adoption.

Project Timeline Requirement

Vendors must provide a detailed and realistic project timeline, including:

- Project phases and sequencing
- Key milestones and deliverables
- Estimated duration for cybersecurity audit, systems integration review, stakeholder engagement, reporting, and validation

Timeline must clearly identify:

- Dependencies on CSH staff availability
- Critical path activities
- Opportunities for early insights or quick wins

Proposals that demonstrate a phased, milestone-based approach, early delivery of high-risk findings, and clear alignment between timeframes and deliverables will be rated more favorably. The timeline must be realistic based on our staffing reality.

Cost Proposal Requirement

Vendors must provide a transparent and detailed cost estimate, including:

- Total proposed cost
- Cost by phase: Phase 1: Cybersecurity Audit and Phase 2: Systems Integration Review, any sub-phases
- Breakdown of labor by role and hourly or daily rates, tools or software used, and any optional services

Required Cost Clarity

Vendors must also specify assumptions used to estimate cost, any variability or optional add-ons, and primary cost drivers such as the number of systems reviewed and interviews conducted.

Team Structure

- Roles and expertise
- Relevant certifications

Risk Identification Approach

- How risks will be surfaced quickly
- Communication cadence

Unauthorized Integration Risk Identification

The vendor must explicitly identify risks associated with unauthorized APIs, integrations, and software usage, including:

- Data exposure through unapproved external connections
- Circumvention of system-of-record controls
- Data integrity issues caused by undocumented data flows
- Increased vulnerability to credential compromise or malicious integrations

These risks must be linked to both technical vulnerabilities and behavior-driven risk factors.

Sample Deliverables

- Redacted audit reports
- Architecture diagrams

Confidentiality and Information Security

Vendors must treat all non-public information received or accessed in connection with this RFP and any resulting engagement as confidential and must use such information solely for the purpose of preparing a proposal or performing services authorized by CSH.

CSH will not provide access to confidential, non-public, proprietary, security-sensitive, or system-specific information until the vendor has executed CSH's nondisclosure agreement.

At a minimum, the selected vendor must:

- Limit access to confidential information to personnel who have a legitimate need to know and who are bound by appropriate confidentiality obligations
- Maintain reasonable administrative, technical, and physical safeguards to protect confidential information from unauthorized access, use, or disclosure
- Promptly notify CSH of any actual or suspected unauthorized access, disclosure, or loss involving confidential information related to this engagement
- Return or securely destroy confidential information at the conclusion of the procurement process or engagement, as directed by CSH, except to the extent retention is required by law
- Comply with any additional confidentiality, data protection, or nondisclosure requirements set forth in the final agreement

Procurement Logistics

Proposal Due Date October 16, 2026

Submission Instructions
Proposals must be submitted electronically in PDF format to cshsystemsrfp@csh.org . Vendors should include the subject line: "CSH RFP Cybersecurity & Systems Integration Review Proposal."

Question and Answer Window
Questions regarding this RFP must be submitted by September 11, 2026. Responses to submitted questions will be provided by September 25, 2026.

Evaluation Criteria

- Independence and objectivity – 20%
- Depth of cybersecurity expertise – 20%
- Integration and data governance capability – 20%
- Practicality and quality of proposed outputs – 20%
- Project approach, timeline, and staffing – 10%
- Cost and overall value – 5%
- Alignment with nonprofit or mission-driven context – 5%

Success Measures

This engagement is successful if:

- Leadership receives a documented view of cybersecurity posture, priority risks, maturity levels, and remediation priorities
- Systems of record, integrations, data flows, and key dependencies are clearly documented
- Reconciliation and data integrity control recommendations are defined and prioritized
- CSH receives a sequenced roadmap with early wins, longer-term improvements, and implementation readiness guidance

CSH reserves the right to request additional information, conduct interviews with selected respondents, and accept or reject any or all submissions. Issuance of this RFP does not obligate CSH to award a contract.

RFP: CSH IT Systems Cybersecurity Audit & Systems Integration Review

Companion Vendor Scorecard for Proposal Review

Evaluation Category	Weight	Score (1–5)	Weighted Score	Reviewer Notes
Independence and objectivity	20%			
Depth of cybersecurity expertise	20%			
Integration and data governance capability	20%			
Practicality and quality of proposed outputs	20%			
Project approach, timeline, and staffing	10%			
Cost and overall value	5%			
Alignment with nonprofit or mission-driven context	5%			
Total	**100%**			

Suggested scoring scale: 1 = Poor, 2 = Fair, 3 = Meets Requirements, 4 = Strong, 5 = Excellent.