NuSummit Cybersecurity

Maclear GLOBAL

WHITEPAPER

Mastering Third-Party Risk in an Interconnected World

An AI-Powered Approach to Regulatory Compliance and Vendor Oversight

Executive Summary

Third-party risk is continuous. Most oversight programs are not.

Regulated organizations manage hundreds to thousands of vendor relationships. Each vendor relationship carries cybersecurity, compliance, and operational risk that changes over time, through security incidents, certification lapses, subcontractor changes, and regulatory actions. Annual assessments and spreadsheet-based tracking cannot keep pace with this reality.

Regulators across the United States and India have made their expectations clear. Vendor oversight must be continuous, evidence-based, and audit-ready. Organizations that cannot demonstrate this face examination findings, enforcement actions, and reputational consequences.

NuSummit Cybersecurity and Maclear Global address this gap through two integrated capabilities. VARAAI, Maclear Global's AI-native GRC platform, automates vendor evidence ingestion, multi-framework control mapping, risk scoring, and continuous monitoring at enterprise scale. NuSummit Cybersecurity provides the governance layer, including operating model design, risk framework definition, regulatory alignment, and program implementation.

Together, we enable organizations to move from periodic, manual vendor oversight to a continuous, defensible TPRM program.

Introduction

Third-party vendors are embedded in the critical operations of most regulated enterprises. Cloud providers, payment processors, IT service providers, and data processors underpin core business functions, and the organizations that rely on them remain accountable for how those vendors handle data, manage security, and comply with applicable regulations.

Most organizations understand this accountability in principle. The challenge is operationalizing it.

Vendor oversight in most organizations today relies on periodic reviews, manual questionnaire dispatch, and fragmented tracking across business units. These methods were designed for smaller vendor ecosystems and less demanding regulatory environments. They do not scale, and they do not produce the continuous, verifiable evidence that regulators now expect.

The structural gaps are consistent across organizations:

- Manual processes that cannot scale to the size of modern vendor ecosystems.
- Fragmented assessments across business units with no unified risk view.
- Point-in-time reviews that do not reflect changes occurring between cycles.
- Duplicated vendor requests across internal functions.
- No visibility into subcontractor and fourth-party risk.
- Evidence that is difficult to aggregate, validate, and present to regulators.
- Tracking and Managing gap/findings

These are not gaps that additional headcount can close. They require a different operating model, one built on automation, continuous data ingestion, and defined governance structures.

The Regulatory Environment for Third-Party Risk

Regulators in the United States and India require organizations to extend their compliance and control frameworks beyond internal systems to cover third-party vendors and their subcontractors. The specific requirements vary by framework, but the underlying expectations are consistent: classify vendors by risk, conduct structured due diligence, monitor continuously, and maintain documentation that can withstand examination.

United States

FFIEC IT & Outsourcing Guidance

Financial institutions must conduct risk-based due diligence, classify vendors by criticality, establish contractual protections, and maintain ongoing oversight programs. Examination workpapers are expected to reflect documented vendor inventories and evidence of active monitoring.

NCUA Supervisory Guidance

Credit unions are held to strict vendor oversight standards, including tiered vendor classification (critical, significant, non-significant), documented due diligence evidence, and board-level reporting on third-party risk exposure.

NYDFS Cybersecurity Regulation (23 NYCRR 500)

Covered entities must assess third parties, embed security requirements in contracts, monitor compliance on an ongoing basis, and report cybersecurity incidents within 72 hours.

HIPAA Security and Privacy Rules

Covered entities must ensure business associates protect protected health information, conduct risk analyses, and execute Business Associate Agreements before data is shared.

CCPA/CPRA: Organizations must ensure vendors comply with consumer data rights, adhere to contractual data handling requirements, and support timely breach notification obligations.

NIST Cybersecurity Framework

Widely adopted as a best-practice baseline across industries, the CSF structures vendor risk management across five functions: Identify, Protect, Detect, Respond, and Recover. It is increasingly used as a cross-framework mapping reference.

India

SEBI Cybersecurity and Cyber Resilience Framework (CSCRF)

Applies to market infrastructure institutions, asset managers, stock brokers, and depositories. Requires cybersecurity controls across six defined domains, with formal evidence submission to SEBI as part of compliance reporting.

Digital Personal Data Protection Act (DPDPA)

Establishes data protection obligations with direct accountability for third-party data processors. Organizations must maintain documented consent structures and data handling controls across their vendor chain.

Across all of these frameworks, the common thread is demonstrable, continuous oversight. Point-in-time assessments and manual evidence collection do not satisfy this standard at scale.

Why Third-Party Risk Is a Continuous Data Problem

Most TPRM programs are built around periodic assessments such as annual questionnaires, scheduled reviews, and certification checks conducted on fixed cycles. This model assumes that vendor risk is relatively stable between reviews. It is not.

A vendor's risk profile can change materially at any point due to:

- Security incidents or data breaches at the vendor or its subcontractors.
- Expiry of SOC 2, ISO 27001, or penetration testing certifications.
- Changes in subcontractor or fourth-party relationships.
- Regulatory actions or enforcement findings against the vendor.
- perational disruptions affecting service delivery or data handling.

These changes occur continuously, and they often occur without notification to the relying organization. The result is that organizations operating on annual assessment cycles may hold outdated risk views for months at a time, with no mechanism to detect or respond to material changes.

At scale, this problem is unmanageable through manual processes. An enterprise managing 500 vendor relationships cannot track certification expiry dates, monitor news events, and review subcontractor changes across that ecosystem without automated systems.

The implication is that TPRM is fundamentally a data management problem. Managing it effectively requires continuous data ingestion, automated analysis, and real-time risk scoring, not periodic questionnaire cycles.

Third-Party Risk Management Domains

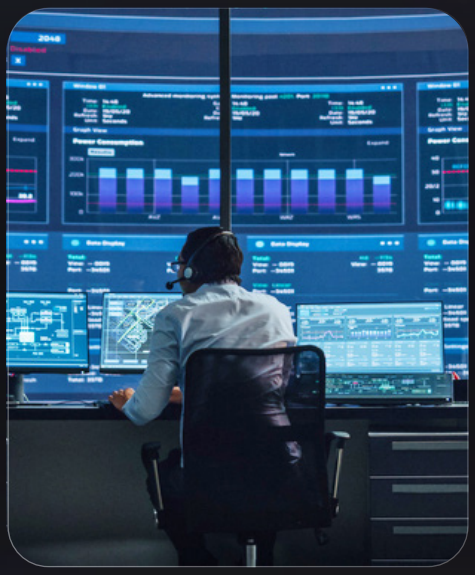
Effective TPRM programs are organized across four operational domains. Each domain has distinct technical and governance requirements. Gaps in either dimension create the weaknesses that regulators most commonly identify during examination.

Vendor Governance and Classification

The foundation of any TPRM program is a complete, accurate vendor inventory with risk-based classification. This means categorizing vendors by criticality, distinguishing those with access to sensitive data or critical systems from those providing lower-risk services, and assigning oversight requirements accordingly. Classification must be maintained as vendor relationships change, rather than being established once at onboarding.

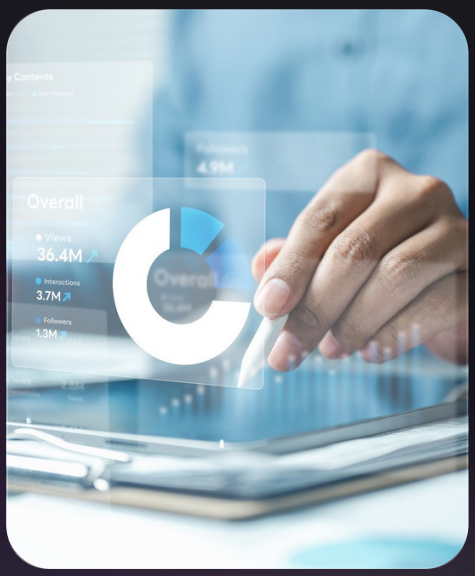
Due Diligence and Assessment

Due diligence requires a structured evaluation of vendor controls supported by independently verifiable evidence. Questionnaire responses alone are insufficient. Effective due diligence requires analysis of SOC 2 Type II reports, ISO 27001/27002 certificates, penetration test results, and other third-party evidence to validate that controls are operating as represented. Assessments must be aligned with the regulatory frameworks applicable to the organization and the vendor relationship.



Continuous Monitoring and Risk Evaluation

Risk scores established at assessment must be updated as conditions change. Continuous monitoring covers certification expiry tracking, external incident monitoring, subcontractor change detection, and regulatory news that may affect vendor risk posture. Risk scores should reflect current conditions, not the state of the vendor at the time of the last formal review.



Audit, Reporting, and Accountability

TPRM programs must produce documentation that supports regulatory examination. This includes complete records of assessment activities and decisions, board-level risk reporting, and evidence packages structured to align with examination workpaper expectations. Documentation must be traceable — regulators expect to see not only what was assessed but how decisions were made and by whom.

VARAAI Platform Architecture and Capabilities

VARAAI is Maclear Global's AI-native GRC platform, purpose-built for third-party risk management in regulated financial institutions. It is designed to automate the core functions of TPRM including evidence ingestion, control mapping, risk scoring, continuous monitoring, and regulatory reporting, at enterprise scale.

The platform is not a traditional risk tool with AI features added. AI is embedded across the full TPRM lifecycle, from vendor onboarding through to board-level reporting.

Core Capabilities

Vendor Onboarding and Risk Classification

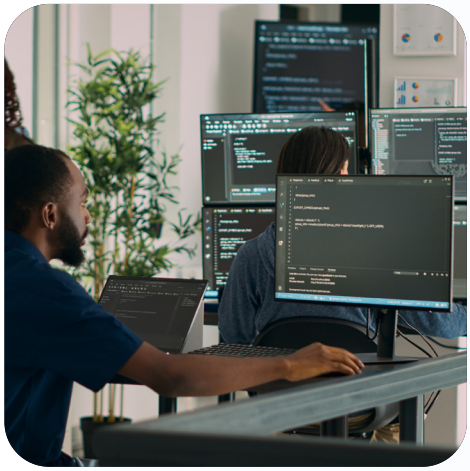
VARAAI captures structured vendor profiles at onboarding, including business context, service scope, data access, geographic footprint, and regulatory exposure. Inherent risk scores are generated automatically based on vendor characteristics and organizational risk appetite. Vendors are classified by tier, aligned to NCUA critical/significant/non-significant categories and equivalent frameworks, and questionnaires are dispatched automatically with control sets mapped to the applicable regulatory requirements for that vendor tier.

AI-Powered Evidence Analysis

VARA AI ingests vendor-submitted evidence, SOC 2 Type II reports, ISO 27001/27002 certificates, penetration test summaries, and questionnaire responses, and extracts control-level findings using AI. The platform performs semantic matching of SOC 2 exceptions and ISO deficiencies to relevant questionnaire controls, identifies scope carve-outs and subservice organization dependencies, generates weighted gap scores by control domain, and compares vendor-asserted controls against the content of independently produced evidence. This shifts the assessment from self-attestation validation to evidence-based control evaluation.

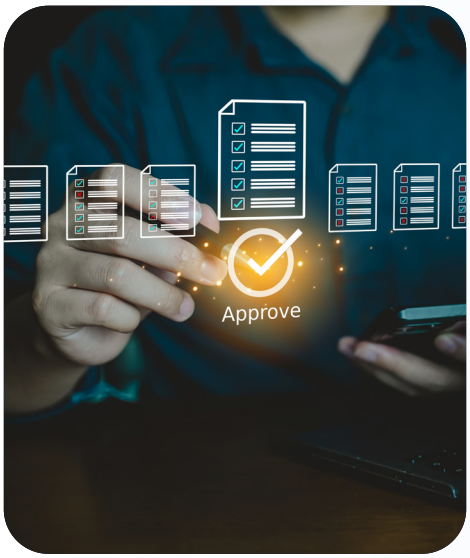
Multi-Framework Control Mapping

VARA AI maintains a unified control library spanning FFIEC, NCUA, NYDFS, HIPAA, CCPA/CPRA, NIST CSF, SEBI CSCRF, DPDPA, and ISO 27001/27002. A single vendor submission, one SOC 2 report, and one ISO certificate are automatically scored against all applicable frameworks simultaneously. This eliminates redundant mapping work and reduces assessment cycle time from days to hours.



Continuous Monitoring

VARA AI maintains a live risk posture for each vendor. The platform tracks SOC 2 and ISO certification expiry windows, ingests regulatory news feeds, and processes incident disclosures. Vendor risk scores are updated dynamically as new information is received. Compliance teams receive automated alerts when a vendor's risk profile changes materially between formal assessment cycles.

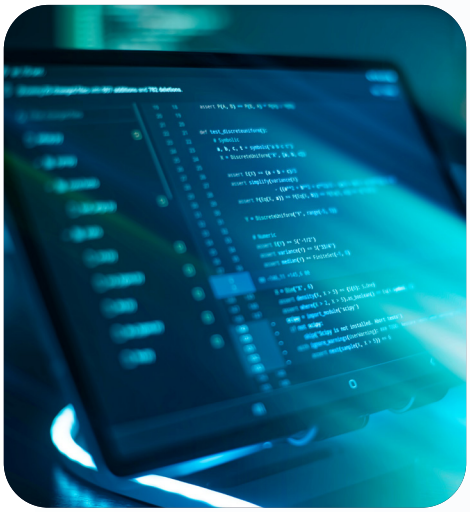


Human Approval Gates

Every AI-generated output, risk scores, control assessments, gap findings, and remediation recommendations are presented as drafts requiring analyst review and explicit approval before finalization. Approved outputs are recorded with full traceability, including reviewer identity and timestamp. This structure ensures that AI-assisted assessments remain attributable to a responsible human reviewer, consistent with regulatory expectations for human oversight in AI-assisted compliance processes.

Regulatory Reporting and Evidence Management

All assessment activity, decisions, and approvals are recorded in a tamper-proof audit trail. VARAAI generates board-ready risk summaries, regulatory evidence packages, and examination workpapers aligned to NCUA, FFIEC, SEBI, and other framework-specific reporting expectations. Reports are generated on demand at each reporting cycle.



Platform Architecture

VARAAI is built on a cloud-native, multi-tenant architecture with full tenant isolation, role-based access controls, and field-level encryption. The platform integrates AI orchestration via Claude AI (Anthropic), a secure data layer with row-level security enforcement, semantic vector search for document analysis and control matching, and serverless workflow execution for agentic TPRM processes. Every action within the platform is logged and auditable.

NuSummit Cybersecurity Advisory Services

A TPRM platform automates process execution. It does not define how risk should be interpreted, how vendors should be classified, or how compliance should be demonstrated to a specific regulator. Those decisions require governance design, and without it, platform outputs remain inconsistent and difficult to defend under examination.

NuSummit Cybersecurity provides the governance and implementation layer that makes VARAAI's capabilities operationally effective and regulatorily defensible. This includes AI-specific services that address both the security of AI systems within vendor environments and the use of AI tooling to accelerate assessment, monitoring, and reporting functions within the TPRM program itself.

Governance and Operating Model Design

NuSummit establishes the ownership and accountability structures that a functioning TPRM program requires. This includes defining vendor inventory ownership, risk classification frameworks, decision rights across business, risk, compliance, and technology functions, and escalation structures for elevated-risk findings. Without this layer, assessments remain isolated activities disconnected from organizational risk management.

Risk Model and Assessment Framework Design

Risk scoring is a policy decision, not a platform configuration. NuSummit defines how vendors are classified, how inherent and residual risk are calculated, and how risk appetite is translated into assessment thresholds. Assessment frameworks are structured to ensure that risk ratings are consistent across vendor types, comparable across time periods, and aligned to applicable regulatory requirements, not dependent on default system settings. Where vendors themselves deploy AI systems, NuSummit incorporates AI-specific risk indicators into the assessment model, drawing on NIST AI RMF and ISO 42001 to evaluate how those systems are governed, monitored, and controlled.

Workflow Design and System Integration

NuSummit designs TPRM workflows that integrate vendor onboarding, due diligence, remediation tracking, and continuous monitoring into a single coordinated process. These workflows are configured within VARA AI and aligned with the organization's existing systems and data flows, ensuring that third-party risk management operates as part of normal business processes rather than as a parallel activity. AI-assisted questionnaire generation, automated vendor response handling via trust catalog smart response, and dynamic risk visualizations are incorporated at the workflow design stage to reduce manual processing and accelerate cycle times.

Regulatory Alignment and Audit Readiness

NuSummit maps TPRM processes to the specific regulatory frameworks applicable to each client, including FFIEC, NCUA, NYDFS, SEBI CSCRF, DPDPA, and others as relevant. Reporting structures, documentation standards, and evidence management practices are designed so that audit-ready evidence is produced as a natural output of the program's normal operation, not compiled separately in advance of examinations. For clients subject to AI-related regulatory expectations, NuSummit maps controls to ISO 42001 and ensures that vendor AI risk is addressed within the compliance reporting structure.

AI Security Advisory Within TPRM

As organizations increasingly rely on third-party vendors that build, operate, or embed AI systems, the TPRM program must account for the risks those systems introduce. NuSummit assesses AI-specific vendor risk across several dimensions: data flow exposure and cross-border transfer risks under GDPR, CCPA, and DPDPA; data exfiltration and leakage risks created by generative AI integrations; model governance and bias risk; and vendor compliance with applicable AI governance standards. This assessment capability is integrated into the standard vendor risk framework rather than treated as a separate workstream.

Implementation and Program Integration

NuSummit manages the implementation of VARA AI within the client environment, including data model configuration, vendor data onboarding, risk model setup, and integration with existing internal systems. The objective is a fully operational TPRM program, not a deployed platform awaiting configuration.

The NuSummit–VARAAI Advantage

TPRM programs that rely on technology without governance produce inconsistent outputs. Programs that rely on governance without technology cannot scale. The NuSummit–VARAAI model integrates both within a single operating approach.

Continuous Risk Visibility

VARAAI replaces point-in-time vendor assessments with continuous risk monitoring across the full vendor portfolio. Risk scores reflect current vendor posture — updated in real time as certifications expire, incidents are disclosed, or regulatory developments occur, rather than the state of the vendor at the last formal review.

Multi-Framework Regulatory Coverage

A single vendor assessment conducted through VARAAI is automatically mapped to all applicable regulatory frameworks. For US financial institutions, this covers FFIEC, NCUA, NYDFS, HIPAA, CCPA/CPRA, and NIST CSF. For Indian financial institutions, SEBI CSCRF and DPDPA requirements are covered simultaneously. This eliminates duplicate assessment work and ensures consistent regulatory coverage.

Evidence-Based Assessment

VARAAI evaluates vendor evidence directly, SOC 2 reports, ISO certificates, and penetration test results, rather than relying on questionnaire self-attestation. Control gaps, scope exceptions, and subservice organization risks are identified through AI analysis of source documents, producing findings that are grounded in independently produced evidence.

Reduced Assessment Burden

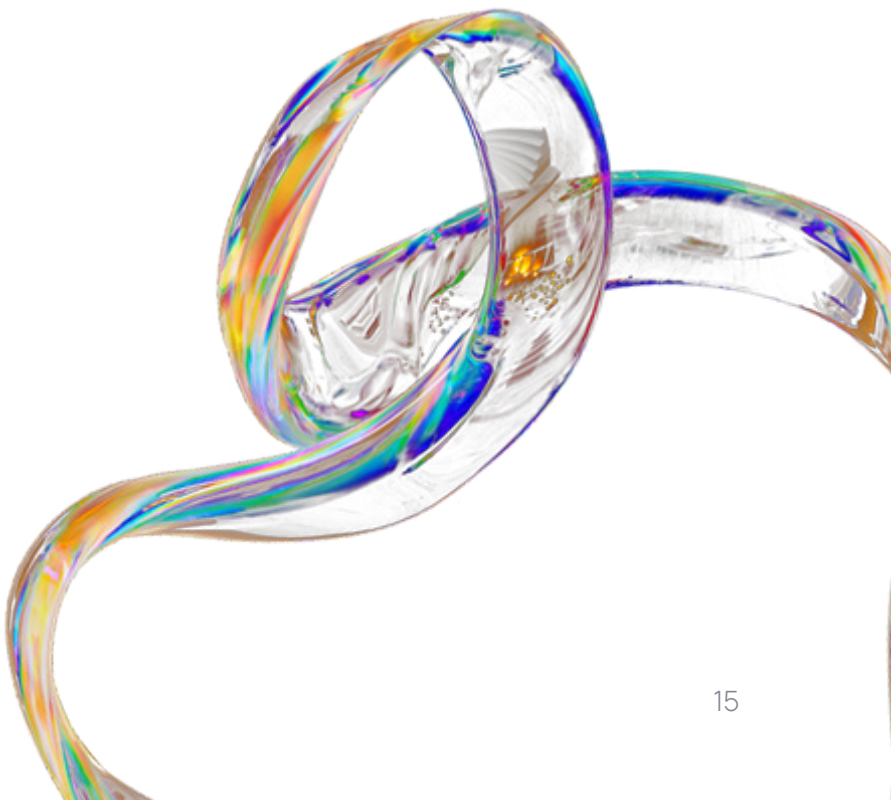
Vendors complete one structured assessment. VARAAI maps responses across all applicable frameworks simultaneously, eliminating the redundant, uncoordinated requests that create friction in vendor relationships and slow down assessment cycles. Assessment cycle time is reduced by up to 70% compared to manual processes.

Audit-Ready Documentation

Every assessment action, approval decision, and risk score change is logged with full traceability. Board-ready reports and regulatory evidence packages are generated on demand, aligned to the specific reporting expectations of applicable frameworks. Documentation is complete as a natural output of program operation — not assembled under time pressure ahead of examinations.

Integrated Governance and Technology

NuSummit's advisory services ensure that VARAAI's outputs are grounded in defined risk models, aligned to regulatory expectations, and integrated into the organization's broader governance structure. The result is a TPRM program where risk evaluation is consistent, decisions are traceable, and compliance can be demonstrated — not just described.



Conclusion

Regulators do not assess organizations on the existence of third-party risk policies. They assess organizations on their ability to demonstrate continuous, evidence-based vendor oversight at scale across their full vendor ecosystem at any point in time.

Manual programs cannot meet this standard. They are too slow, too fragmented, and too dependent on periodic activity to produce the continuous evidence that examination requires.

NuSummit Cybersecurity and Maclear Global address this through an integrated model. VARAAI provides the system capability to manage vendor risk continuously and at scale, while NuSummit provides the governance framework to ensure those capabilities are aligned to regulatory requirements and produce defensible outputs.

Organizations that implement this model gain continuous vendor risk visibility, consistent assessment quality, and audit-ready documentation as standard outputs of their program. In third-party risk management, what cannot be demonstrated cannot be defended.

NuSummit Cybersecurity and Maclear Global support organizations in assessing current TPRM maturity, defining a target operating model, and implementing a scalable program aligned to regulatory expectations across US and Indian jurisdictions. To begin that conversation, contact NuSummit Cybersecurity.

About NuSummit Cybersecurity

NuSummit Cybersecurity helps build and transform cybersecurity postures to enable businesses to mitigate risks. We are a pure-play cybersecurity services company with deep expertise in Identity and Access Management, Risk Advisory, Security Verification, Managed Detection and Response, and Security Engineering services.

Our unique products and services help businesses build and transform security postures while mitigating risks. Our focus is to strengthen security resilience by minimizing the occurrence of attacks, threats, and risks so that you can drive change, innovate, and accelerate growth.

For more information, visit us at cybersecurity.nusummit.com
or write to us at cybersales@nusummit.com

Dallas I Jersey City I Cupertino I Ottawa I Riyadh I Dubai
Mumbai I New Delhi I Bangalore

Follow us at: