Beyond Compliance – Governance That Scales

Turning Regulatory Change into Stronger Governance

Casey Sanderson, CPA | Partner | Forvis Mazars

California Bankers Association Annual Conference | May 2026

forvis mazars

Do you anticipate a reduction in workload because of Part 363 changes?

Opening Poll: Part 363 Expectations

Let's gauge the room — how are you thinking about the threshold changes?

"Who anticipates a reduction in workload because of Part 363 changes?"

- **Live poll**

Why this matters: Many banks see threshold relief as permission to scale back. Today we'll explore whether that's strategic — or risky.

forvis mazars

Threshold Relief ≠ Risk Relief

1

Which controls actually protect the institution, versus simply checking a regulatory box?

2

If we fall below a threshold today but grow past it in a few years, what will it cost to rebuild the infrastructure we dismantled?

3

What will regulators and examiners still expect to see, even without a formal mandate?

FDICIA Part 363: The New Thresholds

Understanding what actually changed in regulatory requirements

Requirement	Old Threshold	New Threshold	Effective Date
Annual Independent Audit	$500M	**$1B**	Jan 1, 2026
ICFR Assessment & Attestation	$1B	**$5B**	Jan 1, 2026

What Regulators Still Expect

Four pillars of governance that examiners continue to evaluate regardless of formal mandates

1.Tone at the Top

Leadership commitment to control culture

2. Control Discipline

Consistent adherence to established processes

3.Risk Escalation

Clear pathways for raising and addressing issues

4.Documentation Standards

Evidence-based governance practices

Exams don't stop caring about control discipline just because the formal attestation requirement moved.

Interactive: Where Are You Now?

Before we dive into the framework, let's see where your institutions stand today.

Poll Question: "Which level best describes your current governance maturity?"

A | **Foundational**
Minimum viable governance: clear ownership, escalation, credible board reporting

B | **Growth**
Repeatable and auditable: documented controls, testing cadence, remediation SLAs

C | **Complexity**
Continuous assurance: monitoring tools, formal ICFR, integrated GRC platforms

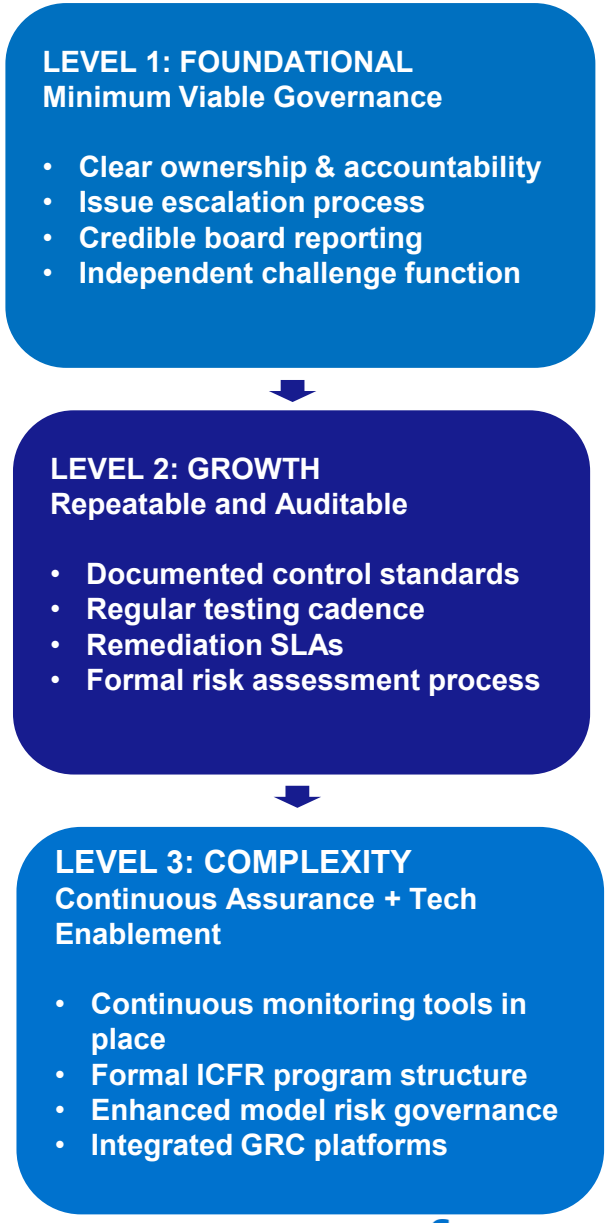
forvis mazars

Which level best describes your current governance maturity?

A Scalable Governance Framework

The Control Governance Ladder – a framework for scaling governance as your institution grows

- Framework provides a clear pathway from foundational controls to advanced automation
- Each level builds on previous capabilities without requiring complete restructuring
- Organizations can assess their current position and identify next maturity steps
- Right-sized governance adapts to growth rather than requiring teardown and rebuild



Right-Sizing Controls: Know the Difference

Protective Controls

- Prevent material misstatement
- Board can explain why it matters
- Failure has business impact
- Tied to specific risk

Performative Controls

- Check a compliance box
- "We've always done it this way"
- Failure has audit finding
- Generic/duplicative

forvis mazars

Translating COSO for the Boardroom

Control Environment:
"Do we reward bad news early?"

Risk Assessment:
"What changed this quarter that makes last year's controls incomplete?"

Control Activities:
"Which controls prevent material issues — and which are theater?"

Info & Communication:
"Are we getting decision-grade info, or dashboard art?"

Monitoring:
"Are issues trending down… or just reclassified?"

forvis mazars

Interactive: COSO Strength Check

Let's assess where your board excels — and where there's room to grow.

Exercise: "Review the five COSO questions we just covered"

Two questions:

- Which question is your board strongest at answering?
- Which question is your board weakest at answering?

The Five COSO Questions:

- Control Environment: "Do we reward bad news early?"
- Risk Assessment: "What changed this quarter that makes last year's controls incomplete?"
- Control Activities: "Which controls prevent material pain — and which are theater?"
- Information & Communication: "Are we getting decision-grade info, or dashboard art?"
- Monitoring: "Are issues trending down… or just reclassified?"

Which question is your board strongest at answering?

Which question is your board weakest at answering?

Clear Roles = Effective Oversight

Function	Board	Audit Committee	Management	Internal Audit
Strategic oversight	R	A	C	I
Control design	I	C	R	A
Control testing	I	I	A	R
Issue remediation	C	I	R	A
Risk assessment	A	R	C	I

R = Responsible, A = Accountable, C = Consulted, I = Informed

What Decision-Grade Reporting Looks Like

Board Control Governance Dashboard – the 10 essential elements boards should be seeing

1.Top 5 Enterprise Risks

With movement vs prior quarter

2.Top Control Failures / Near-Misses

What broke, why, business impact

3.Open Issues Aging

0–30 / 31–90 / 90+ days + owners

4. Repeat Findings Rate

Signals cultural/ownership problems

5.Override Metrics

Policy exceptions, limit breaches

6. Third-Party Risk Heatmap

Critical vendors, SOC issues, concentration

7. Cyber/Fraud KRIs

Phishing loss, Account takeover attempts, anomaly alerts

8. Data Quality Indicators

Recon breaks, manual journals, suspense

9. Change Velocity

Core conversions, product launches, AI rollouts

10.Control Testing Coverage

What's tested, what's not, why

forvis mazars

Control Governance Maturity Check

Self-assessment tool for boards to evaluate their governance maturity across five critical dimensions

Rate your institution on a scale of 1–5 (1 = Ad hoc, 5 = Optimized):

1. Decision-Grade Reporting:
Do we receive actionable, timely governance information?

2. Clear Ownership & Escalation:
Are roles, accountability, and escalation paths defined?

3. Evidence Discipline:
Can we prove our controls work?

4. Tech/Third-Party Visibility:
Do we monitor technology and vendor risks effectively?

5. Issue Remediation Velocity:
Do we resolve problems promptly and track their resolution?

forvis mazars

The $4.5B Bank That Regretted Relief

Case study illustrating the hidden costs of dismantling governance infrastructure

"The lowest-cost path is maintaining a right-sized governance spine — even when thresholds shift."

Jan 2026

Fell below the $5B threshold, dismantled the ICFR infrastructure to "save costs“

June 2027

Rapid growth crossed the threshold again, and scrambled to rebuild systems and documentation

Dec 2027

Spent $2M+ rebuilding what cost $400K annually to maintain

forvis mazars

Interactive: Emerging Risk Readiness

Let's identify where boards feel least prepared for the future

"Which of these emerging risks is your board least prepared to govern?"

A | **AI** (data quality, model risk, third-party accountability)

B | **Stablecoins / GENIUS Act** (new federal framework, operational risk)

C | **Quantum Computing** (cryptographic agility, vendor dependencies)

D | **All of the above** (we're not ready for any of these)

Why this matters: This tees up the importance of* strategic governance *— boards must look beyond compliance to anticipate and prepare for disruptive forces.

forvis mazars

Which of these emerging risks is your board least prepared to govern?

Why AI Governance is Business-Critical

As AI reshapes how businesses operate, real success lies in aligning innovation with accountability, clarity, and trust.

AI is transforming business – from productivity gains to improved customer experiences – but without proper governance innovation quickly becomes exposure. **Organizations need a clear, scalable approach to managing AI risks, aligning with internal values, and meeting evolving regulatory expectations.**

AI governance isn't just compliance, it's organizational confidence. From risk mitigation and control design to model transparency and use case oversight, effective governance enables safe, responsible, impact-driving AI adoption across the enterprise.

Whether you're just starting to formalize your governance, or you need to evolve an existing program to meet new risk, regulatory, or scaling demands, consider the following:

- **Design and build** governance programs that enable safe, effective AI use.
- **Evaluate and enhance** existing frameworks to meet regulatory and business expectations.
- **Assess governance maturity** against leading industry practices and regulations.
- **Operationalize governance** though practical implementation of controls, roles, and oversight.

Strong AI governance turns risk into readiness, and readiness into results.

A Practical AI Governance Starting Point for Community Banks
Phase 1: Visibility

Objective: Create a clear, defensible understanding of **where AI exists, how it is used,** and **what risks it introduces.**

Visibility is the cornerstone of effective AI governance. AI risk cannot be assessed, managed, or controlled without understanding where AI exists, whether formally deployed, embedded within vendor solutions, or used informally.

Activities:

- AI Use Case Identification: Develop an enterprise-wide inventory of AI use cases by engaging businesses, IT, compliance, and vendor management function.
- Lightweight Use Case Profiling: Capture essential attributes for each use case, such as the purpose, impact, type, etc.
- High-Level Risk Triage: Classify existing use cases into broad risk tiers (low/medium/high) based on overall risk level

Sample Deliverables

- Centralized AI Use Case Inventory
- AI Risk Tiering

This creates the foundation to assign ownership and oversight, integrate AI into existing frameworks, and establish guardrails

A Practical AI Governance Starting Point for Community Banks

Phase 2: Accountability, Roles, and Responsibilities

Objective: Ensure AI is governed through clearly defined ownership, oversight, and decision authority

AI governance breaks down if no one is clearly accountable. This risk is mitigated through defining who owns AI use cases, who provides oversight, and how decisions are escalated.

Activities:

- Assign Business Ownership for AI Use Cases

Designate a named business owner for each identified AI use case

- Define Oversight Responsibilities

Clarify the role of risk management, compliance, and legal in AI oversight

- Establish Decision Authority and Approval Thresholds

Define who can approve use cases and clarify what level of review is required

- Define Escalation and Issue Management Protocols

Establishing criteria for escalating AI-related issues or incidents, including who has the authority to pause, modify, or terminate AI use cases

Sample Deliverables

- AI Roles and Responsibilities matrix
- Defined decision authority and escalation thresholds

This positions banks to apply consistent expectations across AI use cases and scale AI adoption without increasing unmanaged exposure.

forvis mazars

A Practical AI Governance Starting Point for Community Banks

Phase 3: Guardrails

Objective: Enable the responsible use of AI by establishing clear, risk-based guardrails that define acceptable use, control, and oversight, without stifling innovation

Once visibility and accountability are established, guardrails provide the structure that allows AI to scale safely, consistently, and in alignment with compliance expectations.

Types of Guardrails:

- Policy-Level Guardrails

Establish clear expectations through acceptable use of GenAI, data handling and confidentiality requirements, prohibited or restricted AI use cases

- Process-Level Guardrails

Embed AI into existing governance workflows with risk-based review thresholds, enhanced third-party due diligence, and change management or issue escalation expectations

- Operational and Technical Guardrails

Ensure AI is used responsibly in practice through human-in-the-loop requirements for material decisions, output review and testing, and access controls and logging

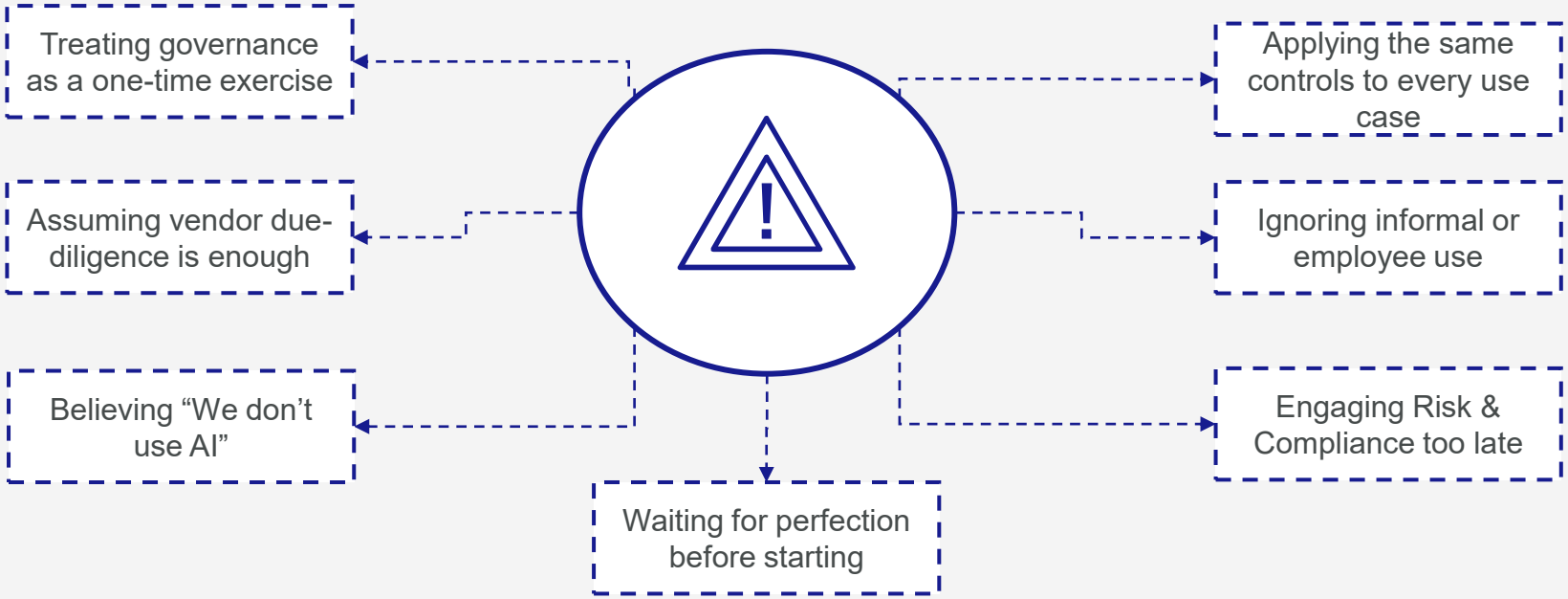
Sample Deliverables

- Acceptable use and guidance documentation
- Defined monitoring and issue management processes
- Control expectations

Where Institutions Often Go Wrong

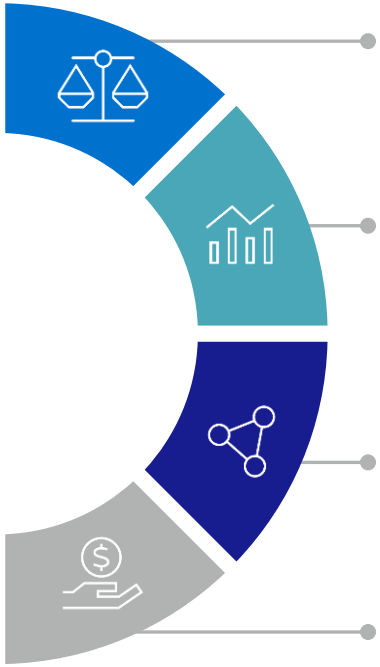
Common AI Governance Pitfalls

Many institutions approach AI governance with good intentions but fall into predictable traps that slow adoption, create blind spots, or introduce unnecessary risk. Understanding these missteps enables more intentional governance design that is pragmatic, scalable, and aligned to enterprise goals.

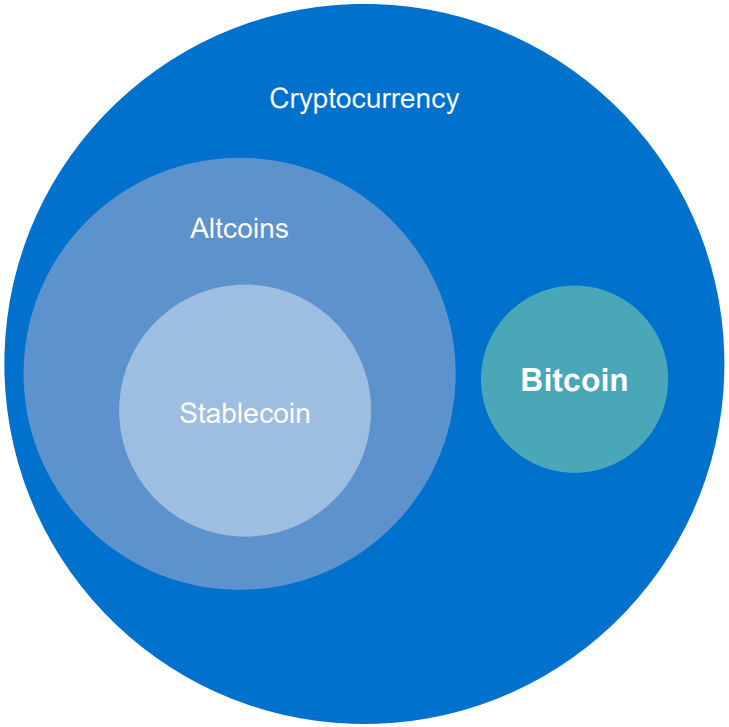


What Is a Stablecoin?

Definition & Purpose



- Cryptocurrency designed to maintain a stable price by tracking the price of underlying assets
- Reduces volatility common in the crypto market & used for payments
- Issued, transferred, & redeemed using cryptography and Distributed Ledger Technology
- "Pegged" to a reference asset (*e.g.*, fiat currency, commodity, or another crypto)



**not exact definition used in the GENIUS Act*

How Can Banks Get Involved?

Potential Pathways

	Build		Buy	
	Launch Your Own Payment Stablecoin	**Launch a Payment Stablecoin With a Consortium**	**White Label a Payment Stablecoin Through Third Party Infrastructure**	**Join a Stablecoin Payment Network via API**
Regulator	Depends: - Federal Banking Agency if subsidiary of IDI - OCC if not an IDI and over $10B - State Regulator if less than $10B	Depends: - Federal Banking Agency if subsidiary of IDI - OCC if not an IDI and over $10B - State Regulator if less than $10B	Depends: - Federal Banking Agency if subsidiary of IDI - OCC if not an IDI and over $10B - State Regulator if less than $10B	Depends: - Federal Banking Agency if subsidiary of IDI - OCC if not an IDI and over $10B - State Regulator if less than $10B
Speed to Market	Long	Variable – depends on consortium formation and approvals	Moderate	Short
Permissible Activities	GENIUS Act-defined services including issuance, redemption, reserve management, etc.	GENIUS Act-defined services shared across consortium members	Customer-facing issuance and redemption; backend managed by third party	Stablecoin payments and settlements via network
Compliance Burden	High – must meet GENIUS Act standards and regulatory oversight	Moderate – shared across consortium	Low to Moderate – Third Party Risk Management, BSA/AML, and Compliance burdens still responsibility of bank	Low to Moderate – Third-Party Risk Management, BSA/AML, and Compliance burdens still responsibility of bank
Scalability	High – but likely dependent on bank's brand and gravitas	High – but likely dependent on consortium's brand and gravitas	Moderate – dependent on third-party capabilities and likely dependent on bank's brand and gravitas	Moderate – limited to payment network's capabilities and no control over branding
Bottom Line	Best for banks with strong internal capabilities, strong brand, and desire to lead in digital payments	Best for banks seeking scale and efficiency through collaboration and strong brand when combined	Best for banks focused on customer experience and speed to market	Best for banks expanding digital payment capabilities without issuing their own payment stablecoin

forvis mazars

Leverage Technology Without Overengineering

Tech maturity curve – using technology to reduce friction without adding unnecessary burden

Foundational

- Excel-based control tracking
- Email-based escalation
- Quarterly manual reviews

Intermediate

- Workflow tools (*e.g.*, SharePoint, Jira, ServiceNow)
- Centralized issue tracking
- Automated reminders for testing/remediation

Advanced

- GRC platforms
- Continuous monitoring and real-time dashboards
- AI-assisted anomaly detection or control testing

Where Governance Must Evolve

1 

AI Governance

- Model risk management
- Algorithmic bias monitoring
- Explainability requirements

2 

Stablecoins / GENIUS Act

- Compliance frameworks
- Reserve monitoring
- Regulatory reporting

3 

Quantum Computing

- Data security threats
- Cryptographic migration
- Infrastructure readiness

forvis mazars

Financial Services

Banking & Credit Unions

The banking sector faces significant regulatory challenges, technological disruption, & shifting consumer habits. In an uncertain & volatile economic environment, adapting business models & embracing disruption is key. Our integrated team of banking & credit union professionals can provide you with the vision & insight to help you navigate a fluctuating landscape.

#5

Ranked fifth in credit union assets audited

1,600+

Team members in the U.S.

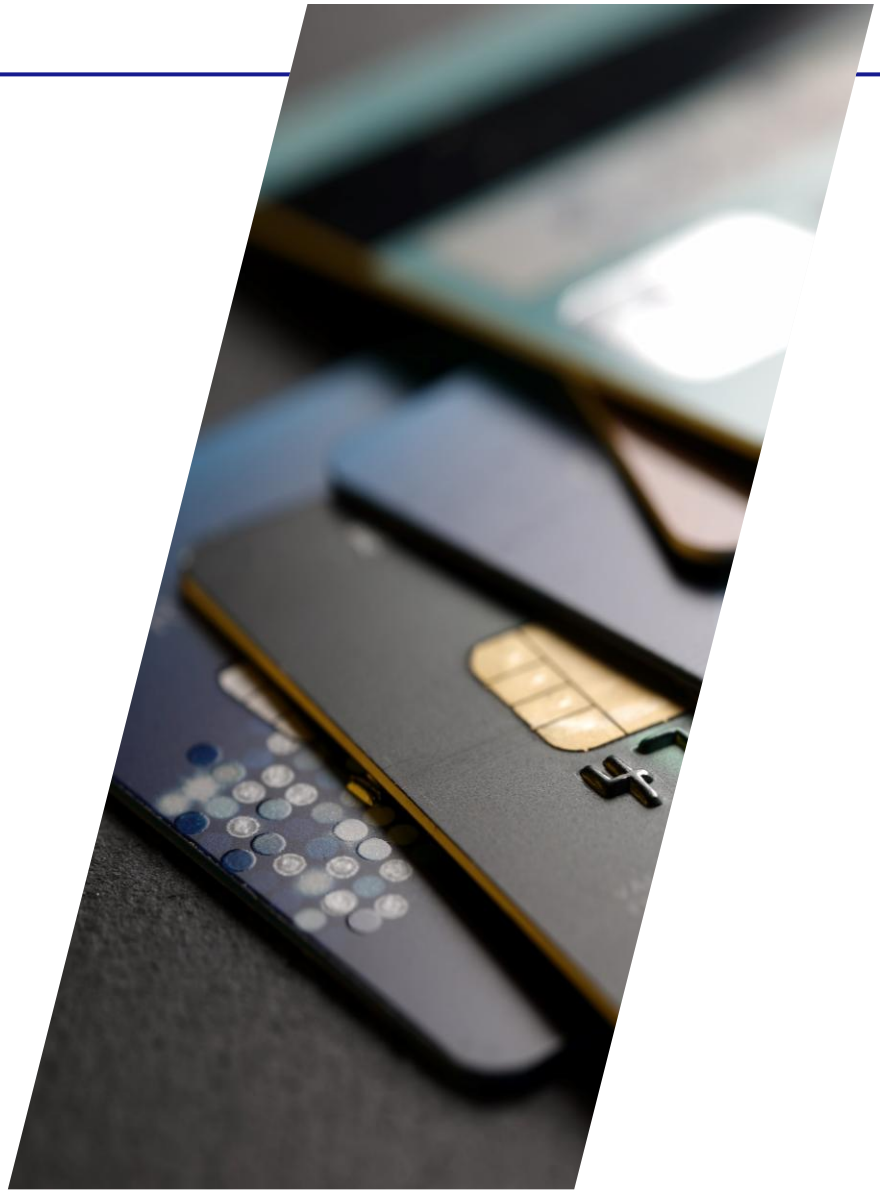
Clients Served by Forvis Mazars in the U.S.

1,900+

Financial Institutions – Banks and Credit Unions

#2

Largest auditor of public banks in the U.S.



forvis mazars

Contact

Forvis Mazars

Casey Sanderson, CPA
Partner
casey.sanderson@forvismazars.com