MOMENT Digital Commerce Readiness Standard v1

Issued by MOMENT — Missouri Mission of Exponential Technologies, a 501(c)(6) business league
Released September 9, 2026

Purpose

The Digital Commerce Readiness Standard (DCRS) certifies that a Missouri business has the operational controls to participate safely in digital commerce — from accepting a stablecoin payment to running live smart contracts, and everything a modern business now sits between: metered APIs, AI agents transacting on its behalf, and revenue that arrives in thousands of small automated events instead of a monthly invoice.

DCRS gives a bank, an enterprise partner, or a state agency a single, checkable answer to three questions: can this business's financial infrastructure handle high-volume automated transactions without breaking; are its controls protected against an AI agent — its own, or a customer's — spending beyond its authority; and can its programmatic treasury and compliance posture be trusted, not just assumed.

Principles

DCRS certifies outcomes, never vendors or protocols. Every requirement is a control or capability a business must demonstrate; no tier requires a named product, custody provider, or payment protocol. A certified business can replace its entire technology stack the next day and remain certified, because it was evaluated against controls, not tools.

Every tier shares non-negotiable prerequisites. No business skips the floor by being large, and none is locked out of it by being small. Depth is available to the businesses that need it; it is never required of the businesses that don't.

Detection and prevention travel together. No tier requires a business to observe a category of risk without also requiring it to control that risk. A business is never asked to instrument autonomous spending it has no authority to halt.

Advisory and assessment are permanently separated. Whoever certifies a business is never the same party paid to help that business prepare. This firewall admits no exception at any tier.

Assessment is uniform and rubric-driven. Every application at a given tier is evaluated against the same published rubric by a designated assessor operating under a written engagement. Certification decisions are issued by MOMENT, not by other businesses.

Evidence requirements rise with the tier. Lower tiers rely on self-attestation; higher tiers require independent, technically qualified review of concrete, verifiable evidence.

The standard is open. Criteria are published in full before application. Certification is available to any Missouri business on identical terms regardless of MOMENT membership.

The Five Tiers

Tier	Name	Requirement	Evidence	Review
1	Digital Ready	Accepts stablecoin payments through a compliant processor; publishes a crypto return/refund policy; staff can explain wallet basics and common scam patterns	Processor agreement or on-chain receipt log; published policy; staff-briefing attestation	Self-attestation, reviewed on application
2	Treasury Aware	Formal internal controls for digital-asset receipts; books reconcile to on-chain activity; documented volatility policy	Documented dual-signature (multi-sig) sweep policy governing transfers from hot wallet to custody; sample reconciliation report; volatility policy	Self-attestation, document review
3	Compliance Ready	AML/CFT risk assessment; trained staff; vendor risk reviewed; **and, for any business with metered or agent-facing infrastructure:** automated telemetry, rate limiting, enforced per-agent spending caps, and a tested kill switch on any	30-day telemetry log; rate-limit configuration; per-agent spending-cap configuration; kill-switch test record; revenue recognition memo for	Designated Assessor review against published rubric — technical and governance competencies, joint sign-off

Tier	Name	Requirement	Evidence	Review
		endpoint or agent with spending authority	usage-based revenue, aligned to ASC 606's variable-consideration guidance (or non-applicability attestation, below)	
4	Institutional Grade	Independent review of digital-asset and automated financial controls; formal agent identity and authorization architecture; named policy owner; ready to transact with public-sector counterparties	Third-party control review report; documented agent authentication and authorization architecture (credential issuance, scoping, delegation chain, provable authorization); named risk owner	Designated Assessor (agent-authentication architecture) plus independent third-party financial review
5	Smart Contract Commerce *(opt-in)*	Live on-chain business logic — escrow, automated settlement, programmable agreements — or equivalent production machine-payable infrastructure; on-chain provenance	Audited, publicly verifiable contract address with documented function coverage; on-chain provenance sample	Designated Assessor (on-chain audit verification) plus third-party review and demonstrated production use

Tier 5 is opt-in, not a default endpoint. A business with no operational need for on-chain logic is a fully certified success at Tier 3 or 4; nothing in DCRS treats that as incomplete. Businesses typically move from Tier 4 to Tier 5 when their need shifts from *controlling* counterparty and settlement risk to *eliminating* it — replacing a clearinghouse or manual reconciliation with trustless on-chain settlement.

That is a business decision each company makes on its own; DCRS certifies correctly on whichever side of that line a business operates.

Why agent controls consolidate at Tier 3

Telemetry detects unauthorized autonomous spending. Spending caps prevent it. A kill switch halts it. Requiring a business to instrument agent activity at one tier while deferring the ability to cap or stop that activity to a higher tier produces a certified business that can watch itself being drained without authority to intervene. All three controls therefore sit together at Tier 3, and all three are conditional on the same trigger: whether the business actually operates metered or agent-facing infrastructure. A business with no such infrastructure carries no additional weight from this consolidation.

Tier 4 retains the architectural requirement that genuinely belongs at institutional grade: a formal agent identity and authorization system — how credentials are issued, scoped, delegated, and proven — reviewed alongside the third-party control assessment. Tier 3 asks whether spending is bounded and stoppable. Tier 4 asks whether every agent's authority is provable and traceable to its source.

Non-applicability and reassessment

A business with no programmatic, API, or agent-driven revenue or spend attests to that fact, and Tier 3's telemetry, rate-limiting, spending-cap, kill-switch, and revenue-recognition requirements are marked not applicable. That status is checked two ways: a business that later exposes a metered API or an autonomous spending agent to production traffic must self-report and resubmit for Tier 3 technical review within 30 days, and every non-applicable certified business additionally receives an automatic annual reattestation check at its renewal date. A lapsed or false non-applicability attestation, however discovered, is a certification integrity violation and is handled through MOMENT's appeals and enforcement process.

Review Model

Tiers 1 and 2 are reviewed by MOMENT staff against the published rubric on the basis of submitted self-attestation and supporting documents.

Tiers 3 through 5 are reviewed by **Designated Assessors** — individuals engaged by MOMENT under a written assessor agreement, evaluated for competence, and bound by confidentiality, conflict-of-interest, and recusal obligations. Two competencies apply:

Technical competency evaluates evidence requiring technical literacy to verify: whether a telemetry log shows what it claims, whether a rate limiter fires under load, whether a spending cap is enforced rather than merely configured, whether a kill switch actually halts spend when triggered, whether an

agent-authorization architecture holds under delegation, whether an on-chain contract matches its claimed function coverage.

Governance competency evaluates documentation and reasoning: AML/CFT risk assessment quality, vendor risk narrative, training records, revenue-recognition methodology.

Both competencies apply a common published rubric with defined pass criteria. An assessor records findings against rubric elements; **the certification decision is issued by MOMENT.** Assessors recommend; MOMENT certifies. No applicant's outcome is determined by another business.

During the pilot phase, assessors may be drawn from the technical and compliance staff of experienced member businesses. Any assessor so drawn is subject to mandatory recusal from applicants who are actual or reasonably potential competitors of the assessor's employer, must sign a confidentiality and conflict agreement covering all applicant material, and may not hold a MOMENT board seat while serving. MOMENT's board may add a paid independent assessor pool as volume warrants, and will do so before certification volume exceeds the capacity of the recusal rules to function.

Standards Committee

A **Standards Committee** drawn from experienced member businesses maintains the assessment rubric, reviews the Standard at least annually, and recommends revisions to the board.

The Standards Committee has **no role in any individual certification decision** and receives no applicant-identifying material. Members shape the standard; designated assessors apply it. This separation is structural and not waivable.

Standard-setting integrity

DCRS is a standard maintained by an association of businesses, some of which compete with applicants. The following controls are therefore binding on every participant in the certification process:

- Certification criteria are published in full and applied uniformly. No applicant is evaluated against unpublished criteria.
- Certification is open to any Missouri business, member or non-member, on identical requirements and identical review.
- No pricing, rate, fee, or commercial-term information of any applicant, member, or competitor is discussed in any Standards Committee, assessor, or board proceeding.
- Any participant with a competitive, financial, or advisory relationship to an applicant recuses from that applicant's matter entirely.
- Every denial, downgrade, or revocation is issued in writing with specific rubric citations and a stated remediation path.

- Every applicant has a right of appeal, decided by parties who took no part in the original decision.

Appeals and enforcement

An applicant may appeal any denial, tier assignment, or revocation within 30 days of written notice. Appeals are decided by an Appeals Panel of MOMENT directors who took no part in the original decision and hold no competitive or advisory relationship to the applicant. Counsel may advise the panel on process only and does not vote. The panel issues a written decision with rubric citations within 45 days. Appeal decisions are final.

Certification may be suspended or revoked for false attestation, failure to maintain a certified control, or failure to self-report a change in applicability status. Revocation follows the same written-notice and appeal process as denial.

Blockchain Requirements by Tier

Tier	**Blockchain required**	**Purpose**
1 — Digital Ready	Yes	Stablecoin payment acceptance
2 — Treasury Aware	Yes	Multi-sig custody and treasury sweep
3 — Compliance Ready	No	Telemetry, rate-limiting, spending-cap, kill-switch, and revenue-recognition controls are protocol-agnostic
4 — Institutional Grade	No	Agent identity and authorization controls are protocol-agnostic
5 — Smart Contract Commerce	Yes	Live on-chain settlement, escrow, and provenance

A business satisfies Tier 3 or 4 by proving the relevant controls exist — a well-instrumented conventional metered-billing stack is sufficient on its own, with no blockchain component required. A business already metering over an on-chain payment rail is not penalized for it, and is not required to reach Tier 5 as a result. Blockchain remains a required, load-bearing part of the standard at Tiers 1, 2, and 5; it is simply not the only path through Tiers 3 and 4, where the operational risk a business carries most often lives in its API and agent infrastructure rather than its custody stack.

Certification, Access, and Renewal

Certification is open to any Missouri business. MOMENT membership is not a prerequisite. Requirements, evidence, rubric, review process, and appeal rights are identical for members and non-members. Non-member applicants pay a certification fee set at or above the member rate; no other term differs.

Certification is issued at the tier for which a business has submitted and had verified the required evidence. Tiers 1 and 2 renew annually by self-attestation. Tiers 3 through 5 renew on a cycle tied to their review method, with non-applicable Tier 3 holders additionally subject to the annual reattestation check described above.

Preparation is unbundled from certification. MOMENT's Digital Readiness Assessment and course catalog are one route to readiness; they are not a prerequisite to apply. A business may prepare through MOMENT programming, a licensed third-party advisor, or entirely on its own, and applies on identical terms in every case. A licensed advisor may help a business assemble its evidence; only a MOMENT-designated assessor evaluates it and only MOMENT issues the credential.

Mentor designation is separate from certification. Tier 4 and Tier 5 businesses may elect to be listed as MOMENT mentor businesses. Election is voluntary, carries no effect on certification status, and declining it carries no penalty.

Alignment with Missouri Policy

DCRS is built to interoperate with, rather than duplicate, existing and pending Missouri programs.

Missouri Angel Investment Incentive. Enacted in the 2026 session as part of the Missouri Innovation, Public Safety and Accountability Act (HB 3231 / HB 2531) and signed by Governor Kehoe, the incentive applies to tax years beginning on or after January 1, 2027. It provides transferable state tax credits of 40–60% of a qualifying cash investment, with enhanced rates for rural counties and certified Missouri Innovation Zones, capped at $6 million annually for 2027 and 2028 and subject to regional allocation across four designated regions including Kansas City. The Missouri Technology Corporation administers the program in coordination with the Department of Economic Development, including annual designation of qualified Missouri businesses, compliance monitoring, and credit allocation.

Designating a business as "qualified" requires MTC to evaluate operational soundness. A Tier 2 or Tier 3 DCRS certification is built to serve as that signal — a documented, independently reviewed operational control posture rather than a narrative claim. **Program rulemaking is underway.** The

definitions being written now determine what evidence MTC and DED will accept; MOMENT's engagement in that process is time-limited and current.

Public-sector transaction readiness. Missouri state agencies, municipalities, and their vendors face an emerging need for vetted guidance on digital-asset treasury handling, agent-mediated procurement, and metered service billing. Tier 4 is built to serve as an operational reference point for that class of counterparty — general public-sector vendor assurance, not contingent on any single piece of legislation.

Legislative activity in this area is ongoing. HB 2080 (2026), which would have established a state Cryptocurrency Strategic Reserve Fund and permitted government entities to accept Department of Revenue–approved digital assets for taxes, fees, and fines, was reported "do pass" from the House Commerce Committee on March 12, 2026 by a 6–2 vote but did not receive a floor vote and did not become law. Reintroduction is anticipated. **DCRS does not depend on its passage.** Should such a measure become law, Tier 4 is positioned to serve as the vendor and agency reference standard without modification.

The standard's tiered structure extends naturally to county- and region-specific cohorts, including Missouri's enhanced-credit Innovation Zones.

Reference Frameworks

DCRS control language draws on established assurance frameworks rather than inventing new evaluative logic from scratch: LEED's universal-prerequisite-plus-tiered-achievement structure; PCI DSS's practice of scaling control requirements to transaction exposure; SOC 2's shift from self-attestation to independent review as stakes rise; the NIST Cybersecurity Framework's maturity-based tiers; and, for revenue-recognition evidence specifically, FASB's ASC 606. Tier 3–5 language describing agent-initiated and machine-metered commerce is informed by current production infrastructure — including Coinbase's x402 protocol and Google's Agent Payments Protocol — cited as reference implementations, not as requirements.

Sources: Missouri Technology Corporation — New Angel Investment Incentive Supports Missouri Startups; LegiScan — Missouri HB 2080 (2026); Projectific — LEED Certification Levels; PCI Proxy — PCI DSS Levels for Merchants and Service Providers; Chainalysis — Inside x402: 100M Agentic Payments on Base; Google Cloud — Announcing the Agent Payments Protocol (AP2); Solvimon — ASC 606 for Usage-Based and AI-Native Businesses.