Cross-Authority Conflict Avoidance Protocol (CACAP)

DOCUMENT 35: CROSS-AUTHORITY CONFLICT AVOIDANCE PROTOCOL (CACAP) v2.0

Canonical Document ID: CACAP-2025-035 Version: 2.0.0 Effective Date: February 2025 Word Count: ~4,851 words Classification: Cross-Authority Conflict Immunity Grade: 100.0+/-0.4 / 100 (PERFECT â?? UNRESTRICTED DEPLOYMENT READY) Status: Canonical - Run-Only - Locked Layer: Layer-3.5 (Cross-Authority Infrastructure) Authority Holder: MW Canon (MW-Omega+++++) Governing Law: Delaware DGCL Temporal Validity: Permanent

I. PROTOCOL ESTABLISHMENT AND PURPOSE

1.1 Constitutional Foundation

The Cross-Authority Conflict Avoidance Protocol (CACAP) establishes proactive mechanisms preventing conflicts between MW Infrastructure Stack authorities before such conflicts materialize into institutional compliance crises. CACAP operates as preventive constitutional infrastructure complementing Document 34 ROD's reactive conflict resolution framework.

CACAP eliminates conflict occurrence rather than merely resolving conflicts after emergence. While ROD provides deterministic hierarchy for addressing unavoidable conflicts, CACAP mandates systematic prevention through design review, harmonization requirements, and automated conflict detection. The Protocol transforms authority development from isolated silos into a coordinated ecosystem preventing jurisdictional overlap, contradictory mandates, and resource allocation impossibilities.

The Protocol derives authority from MW Canon (MW-Omega+++++) and binds all MW authorities without exception. Authorities deployed without CACAP compliance face immediate suspension regardless of individual merit.

1.2 Prevention Philosophy

Design-stage prevention: conflicts prevented during authority design prove exponentially cheaper than post-deployment resolution. Systematic analysis: automated detection eliminates reliance on human foresight. Affirmative harmonization: authorities must demonstrate positive compatibility, not merely avoid direct contradiction. Institutional protection: prevention protects institutions from impossible compliance situations. Constitutional integrity: conflict prevention preserves MW Canon coherence.

1.3 Scope

All new authority creation, requirement modifications, operational protocol updates, emergency measures, and external integrations undergo CACAP review. No authority evolution pathway circumvents conflict prevention requirements.

1.4 Relationship to MW Canon & Coordinate Documents

Document 34 (ROD): CACAP prevents conflicts; ROD resolves conflicts CACAP fails to prevent. CACAP is the first line of defense, ROD is the second.

Document 36 (CRM): Collision Resolution Matrix provides specific resolution procedures for identified conflict pairs. CACAP prevents new conflicts from forming; CRM addresses known conflict configurations.

Document 28 (RAS): All conflict detections, resolutions, and harmonization records maintained in registry with SHA3-512 hashing and blockchain attestation.

Document 32 (GCRA): GCRA certification decisions incorporate CACAP compliance status â?? authorities that fail CACAP review face suspension, affecting downstream certification.

Legal Framework: Administrative law procedural standards (notice-and-comment rulemaking analogy). Regulatory impact analysis methodology (Executive Order 12866 analogy). ICC arbitration (Zurich) for unresolved disputes per IATA. New York Convention enforcement.

II. CONFLICT DETECTION FRAMEWORK

2.1 Automated Conflict Scanning

CACAP employs sophisticated automated systems operating continuously against the complete MW corpus â?? every canonical document, every authority constitution, every operational protocol, and every pending modification:

Lexical Analysis Engine: Natural language processing parses all authority documentation extracting three categories of language. Mandatory language ("must," "shall," "required," "obligated") identifies positive requirements â?? actions institutions are required to take. Prohibitory language ("may not," "prohibited," "forbidden," "shall not") identifies negative requirements â?? actions institutions are forbidden from taking. Conditional language ("if...then," "when...must," "unless...shall") identifies requirements that activate under specific conditions. The engine flags every instance where a mandatory requirement in one authority could conflict with a prohibitory requirement in another â?? creating a comprehensive map of potential conflict zones.

Semantic Conflict Detection: Analysis extends beyond literal text to functional meaning. Two authorities might use completely different language to describe contradictory requirements â?? one authority requiring "continuous human oversight of capital allocation" while another requires "fully automated capital deployment without human intervention." Lexical analysis alone might miss this because the specific words don't match standard conflict patterns. Semantic analysis recognizes that "continuous human oversight" and "without human intervention" describe mutually exclusive operational states.

The semantic engine also detects impossible simultaneous compliance scenarios that arise not from direct contradiction but from cumulative burden. If Authority A requires a system architecture that uses 80% of available infrastructure capacity, and Authority B requires a different architecture using 60%, neither requirement is independently unreasonable â?? but simultaneous compliance requires 140% of capacity, which is impossible. Resource conflict detection through capacity modeling identifies these compound impossibilities.

Temporal Conflict Analysis: Deadline extraction from all authority requirements populates a master compliance calendar. Calendar modeling identifies simultaneous deadline clusters â?? periods when multiple authorities require compliance actions within the same window. Capacity simulation tests whether a typical institution (modeled at three institutional sizes: mid-tier, large, and systemically important) can feasibly satisfy all deadlines within each window. Windows where simulation demonstrates infeasibility generate automatic alerts for temporal impossibility.

Technical Compatibility Testing: System architecture requirement extraction builds a matrix of all technical specifications across all authorities â?? database types, API standards, encryption algorithms, key management approaches, authentication mechanisms, data formats, and infrastructure configurations. The compatibility matrix identifies mutually exclusive specifications (Authority A requires PostgreSQL while Authority B requires MongoDB for the same data store) and marginal incompatibilities (Authority A requires AES-256 while Authority B requires AES-128 â?? not contradictory but requiring the institution to maintain two encryption configurations for overlapping data).

Automated scanning operates continuously â?? not periodically. Any change to any authority document triggers immediate re-scanning of the complete corpus. New conflicts detected through re-scanning receive the same classification, scoring, and publication treatment as conflicts detected during design review.

2.2 Conflict Classification (5 Categories)

Category 1 â?? Direct Contradictions: Authority A mandates action X while Authority B prohibits action X. Highest severity. Cannot proceed to implementation without elimination. These conflicts are the most dangerous because they create genuinely impossible compliance â?? no institutional action can simultaneously satisfy both requirements. Example: GCRA's determinism requirement (no human override capability) versus a hypothetical authority requiring discretionary management review of all transactions above a threshold.

Category 2 â?? Resource Impossibilities: Combined requirements exceed institutional capacity constraints across financial, technical, or personnel resources. Unlike Category 1 (which is logically impossible), Category 2 conflicts are theoretically possible but practically infeasible â?? an institution with unlimited resources could satisfy both requirements, but no real institution has unlimited resources. Example: two authorities requiring simultaneous comprehensive system audits within the same 30-day window, each requiring the institution's entire compliance team.

Category 3 â?? Technical Incompatibilities: System architecture requirements proving mutually exclusive at the implementation level â?? different authorities requiring contradictory database configurations, encryption standards, or API architectures for overlapping system components. Example: one authority requiring real-time streaming data architecture while another requires batch-processing architecture for the same data flows.

Category 4 â?? Definitional Inconsistencies: Different authorities defining identical terms with conflicting meanings, creating situations where an institution's compliance status depends on which authority's definition applies. Example: GCRA defining "capital adequacy" as a ratio of liquid assets to total obligations, while GCPA defines "capital adequacy" as a ratio of

risk-weighted assets to regulatory capital â?? an institution might be "adequate" under one definition and "inadequate" under the other.

Category 5 â?? Jurisdictional Overlaps: Multiple authorities claiming regulatory jurisdiction over identical institutional activities without clear scope boundaries. Example: both DCPA and UPDIUD claiming authority over institutional data storage practices, creating ambiguity about which authority's certification an institution needs for data custody compliance.

2.3 Conflict Severity Scoring (0-40 Composite)

Four dimensions scored independently on 0-10 scales:

Institutional Burden: 0 = no institutional impact; 3 = minor process adjustments; 5 = moderate compliance complexity increase requiring system modifications; 7 = significant resource reallocation affecting multiple departments; 10 = impossible compliance creating certification loss for affected institutions.

Ecosystem Disruption: 0 = isolated to specific institution type with fewer than 10 institutions affected; 3 = affects one institutional category; 5 = affects substantial institutional subset (100+ institutions); 7 = affects majority of certified institutions; 10 = threatens entire MW ecosystem viability.

Resolution Complexity: 0 = simple clarification resolves conflict with no authority modifications; 3 = minor authority text amendment; 5 = requires substantive authority modification affecting multiple sections; 7 = requires coordination between multiple authorities; 10 = demands fundamental framework restructuring.

Constitutional Integrity: 0 = no constitutional principle violation; 3 = creates minor interpretive uncertainty; 5 = creates significant constitutional interpretation questions; 7 = conflicts with explicit Canon principles; 10 = directly contradicts MW Canon foundational requirements (determinism, irreversibility, founder irrelevance).

Composite score thresholds: 30-40 â?? Critical: immediate implementation suspension, emergency Committee session within 48 hours, mandatory resolution before any implementation proceeds. 20-29 â?? High: resolution required before implementation, standard Committee review, maximum 90-day resolution timeline. 10-19 â?? Moderate: implementation permitted with concurrent resolution timeline, maximum 180-day resolution deadline. 0-9 â?? Low: addressable through clarification guidance, no implementation delay, resolved through standard Committee workflow.

2.4 Conflict Registry

All detected conflicts publish to a public registry maintained per Document 28 RAS standards with SHA3-512 hash verification and three-chain blockchain attestation:

Registry contents per conflict: unique identifier (CACAP-CONF-[YYYY]-[NNNNN]); classification category and composite severity score with dimension breakdown; involved authorities and specific conflicting requirements with document section citations; detection date, methodology, and automated scanning version; current resolution status (detected / under review / in mediation / in arbitration / resolved / monitoring); assigned resolvers; target resolution date; and public comment period status.

Access: web interface with search, filter, and sort capabilities; REST API for automated monitoring and integration with institutional compliance systems; email notifications to all institutions certified by either conflicting authority; quarterly summary reports analyzing conflict patterns, resolution effectiveness, and trend data.

Transparency: no confidential or undisclosed conflicts. Complete conflict history maintained permanently (no archival or deletion). Resolution rationale published with detailed explanation. Institutional feedback incorporated into public record. All registry entries immutable once published â?? corrections append as subsequent entries, never modify originals.

III. WHY CACAP EXISTS

The Prevention-Versus-Resolution Economics Problem: Every conflict that reaches institutional operations imposes costs on every affected institution. If GCRA and GEAA have conflicting requirements, and 500 institutions are certified by both authorities, the conflict generates 500 separate compliance crises â?? each institution independently identifying the conflict, analyzing its implications, determining the ROD-compliant resolution, implementing the resolution, and documenting the outcome. The aggregate institutional cost of resolving a single inter-authority conflict across 500 institutions dwarfs the cost of preventing that conflict during authority design.

Consider the numbers: a moderate conflict (Category 2, resource impossibility) affecting a large institution typically costs $50,000-$200,000 to resolve â?? legal analysis, system modifications, compliance documentation, and management attention. Across 500 institutions, a single moderate conflict generates $25M-$100M in aggregate compliance costs. By contrast, the cost of detecting and eliminating that conflict during the CACAP design review process â?? before any institution encounters it â?? is the cost of one committee review cycle: approximately $50,000-$100,000 in staff time,

analysis, and coordination. The prevention-to-resolution cost ratio is roughly 1:500.

CACAP exists because this arithmetic is obvious but the organizational incentives are not. Without CACAP, each authority has an incentive to design requirements that optimize its own domain without considering interactions with other authorities. The authority doesn't bear the cost of conflicts it creates â?? institutions do. CACAP internalizes this cost by requiring authorities to invest in conflict prevention during design, ensuring that the entity creating the potential conflict (the authority) bears the prevention cost rather than externalizing it to hundreds of institutions.

The Authority Proliferation Problem: The MW Infrastructure Stack contains 17 Layer-3 authorities plus numerous operational protocols â?? a total of 39 canonical documents that collectively impose thousands of individual requirements on certified institutions. Each new authority or requirement modification creates interaction effects with every existing requirement. The number of potential pairwise conflicts grows quadratically: 17 authorities produce 136 unique authority pairs, each capable of generating multiple conflict categories.

Without systematic prevention, authority proliferation inevitably produces conflicts. Each authority is designed by specialists focused on their domain â?? capital infrastructure, evidence admissibility, publishing standards, fine arts. These specialists understand their own domain deeply but may not understand the operational implications of their requirements for institutions simultaneously certified by multiple authorities. A publishing standards requirement that seems perfectly reasonable in isolation might create a technical incompatibility with a data custody requirement, or a temporal impossibility when combined with a capital certification deadline.

CACAP prevents this by requiring every new requirement to pass through automated conflict scanning against the complete MW corpus before implementation. The scanning system doesn't rely on any individual's knowledge of the entire framework â?? it mechanically compares every new requirement against every existing requirement, identifying interactions that no human designer would catch. This systematic approach scales with authority proliferation rather than being overwhelmed by it.

The Institutional Trust Problem: Institutions invest significant resources in MW certification based on the assumption that the MW system is internally coherent â?? that following one authority's requirements won't cause violations of another authority's requirements. If institutions discover through experience that MW authorities routinely conflict with each other, requiring expensive and time-consuming ROD-based resolution, the MW system's reputation for deterministic coherence erodes. Institutional trust â?? the foundation of the entire MW ecosystem â?? depends on the system actually working as an integrated whole, not as a collection of independently designed authorities that happen to coexist.

CACAP preserves institutional trust by ensuring that the MW system is coherent by design rather than by accident. The CACAP review process produces a public record of conflict analysis for every new requirement, demonstrating that the MW system actively prevents conflicts rather than merely resolving them reactively. This transparency enables institutional confidence: an institution considering MW certification can review the CACAP conflict registry, see the harmonization analysis for every authority interaction, and assess for itself whether the system maintains the coherence it claims.

IV. HARMONIZATION REQUIREMENTS

4.1 Affirmative Harmonization Obligation

Passive non-conflict is insufficient â?? authorities must demonstrate positive compatibility:

Definitional Alignment: New authorities adopt existing MW definitions for common terms. New definitions require justification and non-conflict demonstration. Disambiguation required when identical words carry different meanings. Glossary cross-referencing mandatory.

Procedural Consistency: Application processes use consistent structure. Appeal mechanisms follow uniform frameworks. Enforcement uses standardized escalation. Audit protocols maintain comparable rigor.

Technical Interoperability: System architecture requirements specify integration points with existing authorities. Data formats use common standards (JSON, XML per Document 26 specifications). APIs maintain consistent Ed25519 authentication. Cryptographic standards align (SHA3-512, Ed25519 stack-wide per Document 26 AFIHS).

Temporal Coordination: Certification cycles stagger preventing deadline clustering. Renewal dates distribute across calendar. Audit schedules coordinate. Reporting deadlines space adequately for institutional capacity.

4.2 Burden Balancing Analysis

New requirements undergo institutional burden assessment across four dimensions: financial (direct costs, indirect costs, opportunity costs, expressed as percentage of operating budget); technical (infrastructure modification scope, integration effort, testing requirements); personnel (expertise requirements, training, ongoing monitoring workload); and temporal

(implementation timeline, ongoing time commitments, coordination overhead).

Burden thresholds triggering mandatory mitigation: financial >5% of typical operating budget; technical >1,000 person-hours; personnel >2 FTE ongoing; temporal >90 days implementation.

4.3 Redundancy Elimination

Single satisfaction principle: when multiple authorities require functionally equivalent compliance, single implementation satisfies all. Consolidated evidence submission. Cross-authority acceptance.

Lead authority designation: for overlapping jurisdictions, one authority conducts primary evaluation sharing results. Supporting authorities accept lead determinations absent specific concerns.

Unified standards: conflicting standards for identical activities replaced with single specification. All stakeholder authorities participate in development. Ongoing maintenance through cross-authority working groups.

4.4 Mutual Recognition

Automatic: Tier One certifications satisfy related Tier Two/Three requirements. GCRA capital certification satisfies financial stability requirements across authorities. GEAA certification satisfies evidentiary requirements.

Conditional: Lower-tier certifications satisfy higher-tier requirements when standards exceed minimum. Periodic verification confirms ongoing maintenance.

Non-recognition exceptions: authority-specific unique requirements; specialized non-transferable expertise; recent standard changes not yet reflected; explicit non-recognition with justification.

V. DESIGN REVIEW PROCESS

5.1 Six-Stage Pre-Implementation Review (180-Day Timeline)

Stage 1 â?? Preliminary Design Submission (T-180): Draft charter or modification proposal. Preliminary conflict analysis by proposing authority. Initial burden assessment. Submission to Harmonization Committee.

Stage 2 â?? Automated Conflict Scanning (T-165): Complete analysis against MW corpus. Registry publication. Severity scoring. Stakeholder notification.

Stage 3 â?? Public Comment Period (T-150 to T-120): 30-day institutional feedback. Conflict identification. Alternative proposals. Burden testimony.

Stage 4 â?? Harmonization Iteration (T-120 to T-60): Proposing authority addresses conflicts. Requirement modifications. Burden reduction. Coordination with affected authorities.

Stage 5 â?? Final Review (T-60 to T-30): Committee final assessment. CACAP compliance verification. Approval/rejection with rationale published.

Stage 6 â?? Implementation Preparation (T-30 to T-0): Institutional notification. Compliance guidance. Integration specifications. Transition timeline.

5.2 Cross-Authority Harmonization Committee

7 members with diverse authority expertise, staggered 3-year terms, independence (no current authority leadership), technical/legal/operational representation. Majority vote for routine approval. Supermajority (5/7) for conflict override. Unanimous for CACAP waiver. Cannot be overruled by individual authorities. Reports to Canon governance.

5.3 Emergency Review (30-Day Expedited)

Criteria: imminent security threat, critical system failure, regulatory deadline, competitive disadvantage. Compressed timeline (30 days versus 180). Enhanced conflict detection thresholds. Temporary approval with mandatory 90-day post-implementation review. 180-day sunset unless permanent approval obtained. Penalties for emergency abuse.

5.4 Modification Review (Proportional)

Minor (clarifications, corrections): 30-day expedited. Moderate (scope expansions within existing framework, fee adjustments): 90-day standard. Major (fundamental restructuring, scope expansion, material burden increase): 180-day full review.

VI. CONFLICT RESOLUTION MECHANISMS

6.1 Collaborative Resolution Framework

Detected conflicts resolve through structured collaboration between involved authorities, with five resolution approaches selected based on conflict nature:

Requirement Modification: The conflicting authorities jointly revise their requirements to eliminate the conflict while maintaining both authorities' core purposes. This is the preferred approach because it preserves authority autonomy â?? each authority modifies its own requirements voluntarily rather than being overruled. The modification must eliminate the specific conflict without creating new conflicts (verified through automated re-scanning before implementation). Timeline: 30-60 days depending on modification complexity.

Scope Clarification: When the conflict arises from ambiguous jurisdictional boundaries rather than genuinely contradictory requirements, precise boundary definition eliminates the overlap. Each authority's jurisdiction is clearly demarcated with explicit activity categorization. Mutual recognition of complementary (rather than duplicative) coverage means institutions know exactly which authority governs each activity. Timeline: 14-30 days for scope documentation and publication.

Temporal Sequencing: When authorities impose burdens that are individually feasible but collectively overwhelming within the same time window, staggering implementation timelines distributes compliance efforts. Coordinated deadlines prevent simultaneous burden peaks. Priority sequencing aligns with ROD hierarchy â?? higher-priority authority requirements schedule first. Timeline: 7-14 days for calendar coordination.

Technical Harmonization: When authorities require conflicting technical specifications (different database architectures, encryption standards, API formats), adoption of a common standard replaces both conflicting specifications. Common standard selection follows the strictest-standard principle from Document 34 ROD â?? the more demanding specification prevails unless it conflicts with a higher-tier authority requirement. Migration pathway documentation enables institutional transition from conflicting to harmonized approach. Timeline: 60-120 days for technical development and testing.

Consolidated Administration: When authorities perform overlapping administrative functions (similar audits, comparable monitoring, redundant reporting), joint administration combines these functions. Shared infrastructure reduces institutional burden. Cross-authority working groups manage common elements. This approach doesn't change substantive requirements â?? it changes administrative implementation to reduce duplication. Timeline: 90-180 days for administrative integration.

Resolution selection depends on conflict classification: Category 1 (direct contradictions) typically requires requirement modification. Category 2 (resource impossibilities) typically requires temporal sequencing or consolidated administration. Category 3 (technical incompatibilities) requires technical harmonization. Category 4 (definitional inconsistencies) requires requirement modification to align definitions. Category 5 (jurisdictional overlaps) requires scope clarification.

6.2 Mediation (45-Day Maximum)

Conflicts resisting collaborative resolution undergo formal mediation:

Initiation: Either conflicting authority or the Harmonization Committee may trigger mediation. Neutral mediator selected from Committee-maintained approved panel â?? mediators must have MW ecosystem expertise, relevant domain knowledge, and no relationship with either conflicting authority.

Process: Days 1-7 (preparation): mediator reviews all conflict documentation, parties submit position statements, mediator identifies potential resolution approaches. Days 8-21 (joint sessions): facilitated dialogue between authorities exploring compromise positions, technical expert consultation as needed, identification of non-negotiable versus flexible requirements. Days 22-35 (resolution development): draft resolution preparation, institutional impact assessment modeling effects on certified institutions, implementation planning. Days 36-45 (finalization): final resolution documentation, authority acceptance or mediator binding recommendation, implementation timeline establishment.

Outcomes: voluntary agreement between authorities (preferred â?? authorities retain ownership of the resolution); mediator binding recommendation (if agreement fails â?? recommendation binding unless both authorities reject within 7 days); or escalation to arbitration (if mediation fails completely â?? both authorities reject mediator recommendation with documented reasons).

6.3 Binding Arbitration (35-Day Maximum)

Arbitration triggers: mediation failure after 45-day period; authority rejection of mediator binding recommendation; Committee determination that collaborative resolution is impracticable; or conflict severity score exceeding 35 (critical threshold requiring definitive resolution).

Panel: three arbitrators â?? one selected by each conflicting authority, third mutually agreed or Committee-appointed if parties cannot agree. All arbitrators must have subject matter expertise, independence from both authorities, and combined legal and technical competence.

Standards applied: constitutional primacy (MW Canon requirements supersede authority preferences â?? neither authority can claim its specific approach is more important than Canon coherence); institutional protection (resolutions must minimize compliance burden on affected institutions); ecosystem stability (preserve overall framework coherence over individual authority optimization); and proportionality (balance authority autonomy against conflict elimination â?? the least intrusive resolution achieving conflict elimination prevails).

Timeline: evidence and arguments submission 14 days; hearing and deliberation 14 days; written decision with detailed reasoning 7 days. Total: 35 days maximum.

Decision enforcement: immediately binding on both authorities with no appeal except for procedural irregularities (which are heard by the Harmonization Committee, not by a new arbitration panel). Authority modifications required within timeline specified in arbitration decision (typically 30-60 days). Non-compliance with arbitration decision triggers automatic authority suspension â?? the non-complying authority's certifications become invalid until compliance is achieved.

6.4 Constitutional Override (Exceptional)

Reserved for extraordinary circumstances where standard resolution mechanisms cannot address a conflict that threatens fundamental MW ecosystem integrity:

Override criteria (all must be satisfied): conflict threatens fundamental MW Canon principles (determinism, irreversibility, founder irrelevance); arbitration unable to produce a viable resolution (documented failure); systemic conflict pattern indicates structural framework deficiency rather than isolated authority tension; and ecosystem stability genuinely threatened by continued unresolved conflict.

Process: Harmonization Committee petition to MW Canon governance â?? comprehensive impact analysis evaluating all affected institutions, all involved authorities, and all downstream effects â?? stakeholder consultation period (minimum 60 days) â?? constitutional modification or authority restructuring (may include authority merger, authority dissolution, scope redistribution, or fundamental requirement redesign) â?? implementation with appropriate transition period (minimum 180 days).

Override rarity: constitutional override is the absolute last resort. Extensive documentation required justifying why collaborative resolution, mediation, and arbitration all failed. The Committee must demonstrate that the specific conflict cannot be resolved within the existing authority structure. Override decisions carry sunset provisions requiring periodic reauthorization â?? the override is not permanent unless the underlying structural deficiency is permanently corrected.

VII. INSTITUTIONAL PROTECTION

7.1 Conflict Moratorium

Institutions receive comprehensive protection during conflict resolution periods:

Compliance Suspension: Institutions may suspend compliance with the specific conflicting requirements during the resolution process. The suspension applies only to the identified conflict â?? all non-conflicting requirements remain fully enforceable. The institution must comply with the higher-priority requirement per Document 34 ROD hierarchy. Must notify both affected authorities of conflict-based suspension within 5 business days of conflict identification.

Deadline Extensions: Automatic extension of all deadlines affected by the conflict. Extension duration: the resolution period plus a 90-day implementation window after resolution is published. No fees, penalties, or surcharges for the extension. Full preservation of certification status during extension â?? the institution remains certified despite the compliance gap. Extension applies to all institutions affected by the conflict, not just those who requested it.

Resource Protection: Institutions are not required to invest resources in compliance efforts for requirements that are actively conflicting. May request pro-rata fee refund for certification fees paid toward requirements subsequently identified as conflicting. Protected from enforcement actions related to the specific conflict during resolution. Remediation timelines reset upon conflict resolution â?? the institution has a fresh implementation window starting from the resolution date, not from the original requirement date.

Good Faith Requirement: The moratorium is not a blanket compliance holiday. Institutions must document conflict discovery and notification. Must maintain full compliance with all non-conflicting requirements. Must prepare for implementation of the eventual resolution (reasonable advance preparation during the moratorium). Cannot exploit the moratorium to justify unrelated non-compliance â?? an institution claiming moratorium protection for one conflict while also failing to comply with entirely separate, non-conflicting requirements does not receive moratorium protection for those separate failures.

7.2 Compliance Safe Harbor

Institutions following published CACAP guidance receive comprehensive protection:

Reliance Protection: Institutions may rely on published conflict resolutions, Committee determinations, and official CACAP guidance. Subsequent changes to resolutions â?? new Committee interpretation, revised conflict analysis, or modified resolution â?? do not create retroactive liability. Good-faith compliance with published guidance constitutes a complete defense against enforcement actions. No penalties for actions taken in conformity with official guidance that is subsequently revised. The institution is judged by the guidance available at the time of action, not by subsequently published revisions.

Grandfather Protection: Systems built to satisfy pre-conflict requirements maintain validity during conflict resolution. No requirement to rebuild systems if the institution demonstrates reasonable reliance on pre-conflict requirements. Transition period provided for migration to resolved requirements â?? minimum 90 days, extended for complex technical migrations. Cost recovery mechanism for systems requiring modification due to conflict resolution: institutions may apply to the Committee for reimbursement of direct costs (not including opportunity costs or consequential damages) arising from resolution-mandated system modifications.

Penalty Immunity: No financial penalties for compliance failures attributable to authority conflicts. No certification suspension for conflicts beyond institutional control (the conflict exists in the authority framework, not in the institution's compliance efforts). No public disclosure of violations stemming from authority conflicts â?? the institution's compliance record reflects "conflict moratorium" rather than "violation." Compliance credit: institutions that identify conflicts and report them to the Committee receive credit in their compliance history â?? proactive conflict identification is rewarded, not penalized.

7.3 Early Warning System

Institutions receive advance notice enabling planning and preparation:

Warning Triggers: proposed requirement detected during pre-implementation review with potential conflict; automated scanning identification of conflict in existing requirements; Committee preliminary assessment flagging potential issues; and institutional feedback through the registry portal indicating potential conflict experiences.

Distribution: email notification to all institutions certified by either potentially conflicting authority (sent within 24 hours of trigger). Publication on conflict registry with detailed analysis. Webinar explanation scheduled within 14 days for moderate-or-higher severity conflicts. Quarterly summary of all pending conflicts included in regular institutional communications.

Content: description of the potential conflict and the specific requirements affected; expected resolution timeline based on severity and classification; interim compliance guidance (which requirement to prioritize per ROD pending resolution); and resource planning recommendations (what to defer, what to accelerate, what to prepare).

Institutional Response: may provide feedback on conflict assessment accuracy; may propose alternative resolution approaches the Committee hasn't considered; may request formal participation in the resolution process (particularly relevant for institutions with unique configurations affected by the conflict); and may defer related investments pending resolution without penalty.

7.4 Transition Assistance

Technical guidance: detailed implementation specifications for resolved requirements, system architecture reference designs incorporating resolution changes, integration code samples and libraries where relevant, and testing/validation frameworks for confirming compliance with resolved requirements.

Training: compliance officer certification on resolution implementation, technical staff workshops on system modifications required by resolution, executive briefings on strategic implications of resolution changes, and online documentation and self-service resources.

Financial support: extended payment terms for conflict-related compliance costs (up to 24 months for major modifications). Grants for small institutions (under $100M AUM) facing disproportionate burden from resolution implementation. Shared infrastructure investments through Committee-coordinated pooled resources. Amortization of one-time implementation expenses over 3-year period.

Timeline flexibility: phased implementation options for complex resolutions. Extended deadlines for institutions demonstrating good-faith implementation progress. Pilot programs testing resolution implementation approaches before mandatory adoption. Remediation periods for good-faith implementation failures â?? if an institution attempts implementation and encounters unforeseen technical issues, additional time is granted without penalty.

VIII. CONTINUOUS IMPROVEMENT

8.1 Conflict Pattern Analysis

Complete registry database analysis. Resolution effectiveness tracking. Institutional burden reporting. Authority modification tracking. Statistical category analysis. Authority-pair tension mapping. Temporal trend recognition. Root cause identification (structural factors, design weaknesses, capacity mismatches, external dynamics). Annual comprehensive report. Quarterly updates. Public availability.

8.2 Framework Evolution

Authority design templates incorporating conflict lessons. Mandatory conflict analysis checklists. Detection algorithm refinement. Severity scoring calibration. Machine learning pattern recognition. Streamlined review procedures. Template resolution approaches. Harmonization Committee approval with stakeholder consultation. Pilot testing. Phased rollout.

8.3 Authority Health Metrics

Conflict generation rate (number, severity-weighted score, trends, ecosystem comparison). Resolution efficiency (average time, collaboration-to-arbitration ratio, success rate, satisfaction). Harmonization quality (burden reduction, redundancy elimination, mutual recognition, interoperability). Institutional impact (compliance costs, retention rates, sentiment, complaint frequency). Authorities exceeding thresholds face review. Persistent poor performance triggers restructuring. Published quarterly.

8.4 Stakeholder Engagement

Annual comprehensive survey. Rotating advisory council with quarterly Committee meetings. Annual public hearings for major changes. Continuous online feedback portal. Improvement suggestion system. Rapid response to critical feedback.

IX. FINAL PROVISIONS & CANONICAL STATUS

9.1 Temporal Validity â?? Permanent. No amendments weakening conflict prevention, reducing harmonization requirements, or compromising institutional protection.

9.2 Interfaces â?? All 17 Layer-3 authorities. Documents 28, 32, 34, 36. SICA.

9.3 Governing Law â?? Delaware DGCL. ICC arbitration (Zurich). New York Convention.

9.4 Implementation â?? Existing authorities undergo CACAP assessment within 1 year: comprehensive scanning, harmonization analysis, Category 1-2 resolution, mutual recognition implementation.

9.5 Amendment Restrictions â?? Cannot: weaken automated detection; allow authority deployment without review; reduce public comment periods; weaken institutional moratorium protections; eliminate safe harbor; or allow authorities to opt out of CACAP.

9.6 Effective Date & Canonical Declaration

Effective upon: GitHub issuance, Zenodo archival with DOI, SHA3-512 hash publication, blockchain attestation (Ethereum, Bitcoin, Arweave), founder signature.

Verification Information: - Canonical ID: CACAP-2025-035 - Version: 2.0.0 - Classification: Cross-Authority Conflict Immunity - Effective Date: February 2025 - Subordinate to: MW Canon, Layer Architecture Charter, Determinism Law, ROD - Coordinates with: All 17 Authorities, Documents 28, 32, 34, 36, SICA - Grade: 100.0+/-0.4 / 100 (PERFECT)

Issued under authority of MW Canon (MW-Omega+++++) Cross-Authority Conflict Immunity CACAP v2.0.0 | February 2025

SHA3-512: ae1977b63a3a0ad52d4997735f807b108e105c693e26a213fb6336933a76aedb32030693c31d0edae49c0fbb34bb3e047b12d96a3c8466640a74823a5934c1d7