



COGNITIVE MODE OPERATING SYSTEM STANDARDS BOARD (CMOS-SB)

CMOS-SB: Governing the Human-Machine Layer

*The Complete Framework for Emotional Infrastructure Safety,
Cognitive Mode Governance, and Population-Level Wellbeing*

Document Title	CMOS-SB Flagship Master Document
Document ID	CMOS-SB-FMD-001
Version	1.0
Publication Date	June 9, 2026
Effective Date	September 9, 2026, pending ratification by the CMOS-SB Board of Directors
Next Review Date	September 9, 2027
Issued by	Cognitive Mode Operating System Standards Board (CMOS-SB)
Hosted by	Sugar Sands Publishing LLC, Pensacola, FL
Author	Isabelle Anne Thompson
ORCID	0009-0002-7213-3235

Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.

Executive Summary

The Cognitive Mode Operating System Standards Board (CMOS-SB) is the world's first standards body governing the Human-Machine Layer — the interface domain at which digital systems interact with, influence, and shape human emotional states and cognitive modes. This document presents the complete CMOS-SB framework: its scientific foundations, governance architecture, standards canon, operational doctrine, and real-world implementation model. It serves as the authoritative master reference for all stakeholders engaging with CMOS-SB standards, the frameworks they govern, and the ecosystem they anchor.

CMOS-SB was founded and architected by Isabelle Anne Thompson, Founder and Principal of Sugar Sands Publishing LLC (SSP) and Founder of Sugar Sands Philanthropies Inc (SSPhi), based in Pensacola, FL. CMOS-SB is hosted by SSP and operates independently under its governance architecture. The intellectual property underlying the entire ecosystem — including Emotional Epidemiology, the Susceptibility-Transmission-Collective Resilience (S-R-C) Model, Cognitive Mode OS Theory, CMOS-SB, the Configuration Management Plan for Human Cognition (CMP-HC), and Joy Tracker — is owned by Sugar Sands Publishing LLC and stewarded by Isabelle Anne Thompson as architect and standards steward.

The CMOS-SB ecosystem is built on five interlocking lines that, together, constitute the world's first complete framework for emotional infrastructure safety and cognitive mode governance at scale:

- **Emotional Epidemiology** — the scientific discipline that explains *what is happening* at the population level with respect to emotional states, propagation, and systemic impact.
- **The S-R-C Model** — the theoretical framework explaining *how* emotional dynamics operate through Susceptibility, Transmission Rate, and Collective Resilience.
- **CMOS-SB** — the standards body that defines *what responsible systems should do* about these dynamics through governance, safeguards, and requirements.
- **CMP-HC** — the operational doctrine defining *how to implement and audit* those responsibilities in practice.

- **Joy Tracker** — the reference implementation that proves *the ideas can operate in the real world*, generating evidence and validating standards in practice.

The five CMOS-SB Governance Spine standards — the Emotional Infrastructure Safety Standard (EISS), Cognitive Mode Stability Standard (CMSS), Emotional Transparency and Disclosure Standard (ETDS), Emotional Data Consent and Privacy Standard (EDCPS), and Population-Level Emotional Risk Monitoring Standard (PERMS) — collectively establish baseline safety requirements, cognitive stability protections, mandatory transparency obligations, consent and privacy rights, and population-level monitoring protocols for any system that interacts with, influences, or responds to human emotional states and cognitive modes.

The CMOS-SB framework is designed for adoption by technology developers, platform operators, healthcare organizations, public institutions, researchers, and policy bodies. It is science-grounded, independently governed, publicly accountable, and explicitly oriented toward the protection of human dignity, relational integrity, cognitive stability, emotional wellbeing, and collective resilience. This Flagship Master Document — CMOS-SB-FMD-001, Version 1.0, effective June 9, 2026 — is the complete and authoritative articulation of that framework in a single publication.

About the Founder and Architect

Isabelle Anne Thompson is the Founder and Principal of Sugar Sands Publishing (SSP), the Creator and Architect of the CMOS-SB framework, the Steward of CMOS-SB Standards responsible for conceptual integrity and long-term evolution, and the Founder of Sugar Sands Philanthropies (SSPhi). All intellectual property associated with Emotional Epidemiology, the S-R-C Model, Cognitive Mode OS Theory, CMOS-SB, CMP-HC, Joy Tracker, and all related frameworks, characters, and standards is owned by Sugar Sands Publishing LLC and stewarded by Isabelle in her role as architect and standards steward. CMOS-SB is hosted by SSP and operates independently under its governance architecture; SSPhi serves as the philanthropic affiliate supporting the public-interest mission of the ecosystem.

Table of Contents

Executive Summary

About the Founder and Architect

Part I — Introduction: The Case for Human-Machine Layer Governance

- 1.1 The Human-Machine Layer
- 1.2 The Problem Emotional Infrastructure Solves
- 1.3 CMOS-SB: Purpose, Mission, and Mandate
- 1.4 Legal Structure and Hosting

Part II — Scientific Foundations

- 2.1 Emotional Epidemiology — The Science of Population-Level Emotional Dynamics
- 2.2 The S-R-C Model — A Population-Level Framework
- 2.3 Cognitive Mode OS Theory — The Governing Layer
- 2.4 Zero Trust Evolution — The Cybersecurity Parallel

Part III — The CMOS-SB Ecosystem

- 3.1 The Five-Line Architecture
- 3.2 The Governance Spine — Five Standards Pillars
- 3.3 Reference Architecture RA-1.0

Part IV — Standards Canon

- 4.1 EISS v1.0 — Emotional Infrastructure Safety Standard (CMOS-SB Standard 1001)
- 4.2 CMSS v1.0 — Cognitive Mode Stability Standard
- 4.3 ETDS v1.0 — Emotional Transparency & Disclosure Standard
- 4.4 EDCPS v1.0 — Emotional Data Consent & Privacy Standard
- 4.5 PERMS v1.0 — Population-Level Emotional Risk Monitoring Standard

Part V — CMP-HC: Operational Doctrine

- 5.1 What CMP-HC Is
- 5.2 CMP-HC Technical Architecture — Six Primary Components

- 5.3 CMP-HC Compliance Domains — Six Domains
- 5.4 Control Architecture — Sample Control Mappings
- 5.5 CMP-HC ↔ CMOS-SB Translation Matrix

Part VI — Safeguard Implementation

- 6.1 Safeguard Design Pattern Set (CMOS-SB v1.0)
- 6.2 Closed-Loop Control Effectiveness System

Part VII — Governance Structure

- 7.1 Founding Charter — Constitutional Framework
- 7.2 Governance Architecture — Multi-Body Structure
- 7.3 Standards Development Process (SDP)
- 7.4 Independence Protections
- 7.5 Certification and Compliance Registry

Part VIII — Regulatory and Cross-Framework Alignment

- 8.1 Regulatory Coverage Map
- 8.2 NIST SP 800-53 Alignment
- 8.3 SOC 2 Type II Alignment
- 8.4 HIPAA/HITECH Alignment

Part IX — Joy Tracker: Reference Implementation

- 9.1 Purpose and Role
- 9.2 How Joy Tracker Validates the Ecosystem
- 9.3 Lessons from the Field

Part X — Implementation Roadmap

- 10.1 For Organizations Seeking Compliance
- 10.2 For Standards Bodies and Regulators
- 10.3 For Researchers and Academics

Appendices

Appendix A — Glossary of Terms

Appendix B — Standards Registry

Appendix C — CMP-HC Domain Reference

Appendix D — Translation Matrix Summary

Appendix E — Traceability Schema Summary

Appendix F — Document Control

PART I

Introduction: The Case for Human-Machine Layer Governance

1.1 The Human-Machine Layer

We are living through a foundational transition in the relationship between human beings and the digital systems that surround them. For most of the history of computing, human-machine interaction was primarily instrumental: a person issued a command, a system returned a result. The human was the agent. The machine was the tool. The interface between them was transactional, bounded, and legible.

That model no longer describes the reality of the systems being deployed at scale today. Digital systems increasingly read emotional signals — through text sentiment, voice tone, behavioral pattern analysis, physiological inputs, and interaction timing. They modulate cognitive load — through interface design, content pacing, notification architecture, and adaptive response generation. They influence attention — through recommendation algorithms, engagement optimization, and ambient prompting. They shape relational dynamics — through mediated communication, social signal processing, and relationship-spanning interaction histories. They alter emotional trajectories — through the cumulative weight of what they surface, amplify, suppress, and withhold. And they do all of this in real time, at a scale that encompasses billions of people simultaneously, and at a speed that outpaces any human regulatory response.

These systems operate at the intersection of engineering and neuroscience, of software design and social psychology, of product development and public health. They sit, in short, at what this document names the **Human-Machine Layer**: the interface domain where digital systems interact with, influence, and shape human emotional states and cognitive modes.

The Human-Machine Layer is not a metaphor. It is a technical and social reality with measurable properties, definable boundaries, identifiable risk surfaces, and observable failure modes. It is the layer at which a platform's design choices become emotional exposures for users. It is the layer at which an artificial intelligence (AI) system's adaptive responses become cognitive load events. It is the layer at which a notification architecture becomes an attentional control system. And it is, critically, the layer at which population-level emotional dynamics emerge — where individual interactions aggregate into collective emotional states, where susceptibility and transmission combine to produce drift, contagion, and mode collapse at scale.

Until now, this layer has been ungoverned. Traditional technology safety frameworks address hardware reliability, data security, and system uptime. They do not address emotional impact, cognitive mode safety, or population-level emotional risk. Traditional public health frameworks address physical disease, environmental hazards, and behavioral risk factors. They have not yet been extended to the domain of digital emotional influence. Traditional professional ethics frameworks address individual practitioners in defined relationships. They do not scale to the ambient, always-on, population-spanning interactions that characterize modern digital systems.

The absence of governance at the Human-Machine Layer is not an oversight — it reflects the genuine novelty of what these systems have become. But novelty is not an exemption. The speed with which these systems have been deployed, the depth of their integration into daily human life, the asymmetry of information and power between system operators and the populations they affect, and the measurable evidence that emotional harm at scale is a real and present consequence of current design practices together constitute a compelling and urgent case for structured governance.

CMOS-SB was created to provide that governance. This document is its authoritative articulation.

1.2 The Problem Emotional Infrastructure Solves

The concept of **emotional infrastructure** refers to the technical and relational systems that mediate emotional and cognitive experience at scale. Just as physical infrastructure — roads, power grids, water systems — mediates the physical conditions of human life, emotional infrastructure mediates the cognitive and emotional conditions of human life. It is the substrate through which emotional experiences are shaped, transmitted, amplified, suppressed, and structured.

Emotional infrastructure is not inherently digital, but today's most consequential emotional infrastructure is. Social media platforms, AI-powered communication tools, recommendation systems, adaptive learning environments, digital health interfaces, and workplace productivity systems collectively constitute an emotional infrastructure that touches virtually every dimension of contemporary human experience. They determine what information people encounter, how they encounter it, at what pace and volume, with what emotional framing, and in what relational context.

Physical infrastructure, financial systems, and public health systems have all been recognized as domains requiring structured safety governance. Roads are governed by traffic codes, engineering standards, and crash-safety requirements. Financial systems are governed by capital requirements, transparency standards, and systemic risk monitoring. Public health systems are governed by epidemiological surveillance, intervention protocols, and population-level safety requirements. In each of these domains, the recognition that scale creates systemic risk — that individual interactions aggregate into population-level outcomes that require governance beyond individual choice — drove the development of standards bodies, regulatory frameworks, and safety requirements.

The same logic applies to emotional infrastructure. The absence of structured governance at the Human-Machine Layer has produced predictable consequences: no standardized method for defining cognitive baselines against which system behavior can be evaluated; no structured approach to managing emotional interfaces in ways that protect rather than exploit user vulnerability; no mechanism for identifying cognitive-mode transitions and ensuring that system behavior responds appropriately; no framework for mitigating cognitive drift in environments designed to maximize engagement; and no protocol for preventing emotional overload in populations already operating under conditions of elevated susceptibility. These are not hypothetical risks. They are observable, measurable, and addressable — which is precisely what CMOS-SB exists to do.

1.3 CMOS-SB: Purpose, Mission, and Mandate

Mission Statement

The mission of CMOS-SB is to safeguard emotional-infrastructure safety by developing, publishing, and maintaining standards that ensure systems interacting with human cognition and emotion operate in ways that protect human dignity, relational integrity, cognitive stability, emotional wellbeing, and collective resilience.

Jurisdictional Scope

CMOS-SB standards apply to any digital system — including AI-enabled platforms, social and communication platforms, adaptive learning systems, digital health applications, consumer technology, and enterprise tools — that interacts with, influences, or responds to human emotional states or cognitive modes at any scale of deployment.

Authorized Functions

- Define and publish standards governing the Human-Machine Layer
- Establish certification requirements and maintain the Certification Registry
- Issue interpretive rulings providing formal clarification of standards
- Maintain the Standards Registry with complete version history
- Convene committees, expert panels, and working groups
- Administer the public comment process and publish responses
- Monitor post-publication implementation and publish findings

What CMOS-SB Does Not Do

Scope Limitations — Authoritative Statement

CMOS-SB does **not** regulate individual organizations, enforce compliance through legal or governmental mechanisms, engage in commercial activities of any kind, endorse or certify specific

products or services, serve as a lobbying or advocacy organization, or issue binding legal requirements. CMOS-SB standards are voluntary governance instruments. Compliance is chosen; it is not compelled. This independence is a feature, not a limitation.

1.4 Legal Structure and Hosting

CMOS-SB is constituted as an independent standards body hosted by Sugar Sands Publishing LLC, a limited liability company incorporated in Florida and headquartered in Pensacola, FL. Sugar Sands Publishing LLC provides legal entity status, administrative and operational support, and publication infrastructure for CMOS-SB. It does not influence standards content, participate in governance decisions, or determine compliance outcomes.

The separation of the hosting entity from the governance function is a structural independence protection built into the CMOS-SB Founding Charter. Standards content is determined solely by the CMOS-SB Standards Committee, subject to Board of Directors ratification and mandatory public comment. No employee, officer, or affiliate of Sugar Sands Publishing LLC may hold a governance role that creates a conflict of interest with their hosting responsibilities, and no commercial interest of Sugar Sands Publishing LLC may be advanced through standards decisions. Sugar Sands Philanthropies Inc (SSPhi) serves as the philanthropic affiliate supporting the public-interest mission of the ecosystem and does not hold governance authority over standards development.

PART II

Scientific Foundations

2.1 Emotional Epidemiology — The Science of Population-Level Emotional Dynamics

Emotional Epidemiology is an interdisciplinary scientific framework for understanding how emotional states emerge, propagate, and stabilize within human populations. Introduced by Isabelle Anne Thompson (Sugar Sands Publishing LLC / Sugar Sands Philanthropies Inc; ORCID: 0009-0002-7213-3235; DOI: 10.5281/zenodo.20314466), Emotional Epidemiology draws from psychology, sociology, public health, network science, and systems theory to construct a rigorous, empirically grounded science of population-level emotional dynamics.

The central thesis of Emotional Epidemiology is that emotional states are not merely individual psychological phenomena. They are systemic events with population-level properties. Emotions spread. They transmit from person to person through direct interaction, mediated communication, shared environmental exposure, and network effects. They respond to conditions — environmental, relational, and infrastructural — in ways that are consistent, predictable, and measurable. And they exhibit system-level behaviors: cascading effects, equilibrium states, tipping points, self-reinforcing loops, and recovery dynamics that can be described, modeled, and — critically — governed.

This framework positions emotional states as public health phenomena in the same sense that infectious diseases are public health phenomena: subject to population-level surveillance, systemic risk assessment, intervention design, and outcome evaluation. The key finding of Emotional Epidemiology is that emotional states follow predictable spread patterns, respond to environmental and network conditions, and exhibit measurable system-level behaviors that can be characterized through empirical observation, modeled through formal theoretical frameworks, and mitigated through deliberate design. This finding is the scientific foundation upon which all CMOS-SB standards are built.

Emotional Epidemiology identifies three governing forces of population-level emotional dynamics — Susceptibility, Transmission Rate, and Collective Resilience — formalized in the S-R-C Model (see Section 2.2). It also identifies the primary risk surfaces at which population-level emotional harm occurs: digital emotional infrastructure, mediated relational environments, and AI-adaptive interaction systems — precisely the systems governed by CMOS-SB standards. The long-horizon field observation methodology used to develop and validate Emotional Epidemiology is described in the preprint published at DOI:

10.5281/zenodo.20314466 and is further elaborated through the Joy Tracker reference implementation described in Part IX of this document.

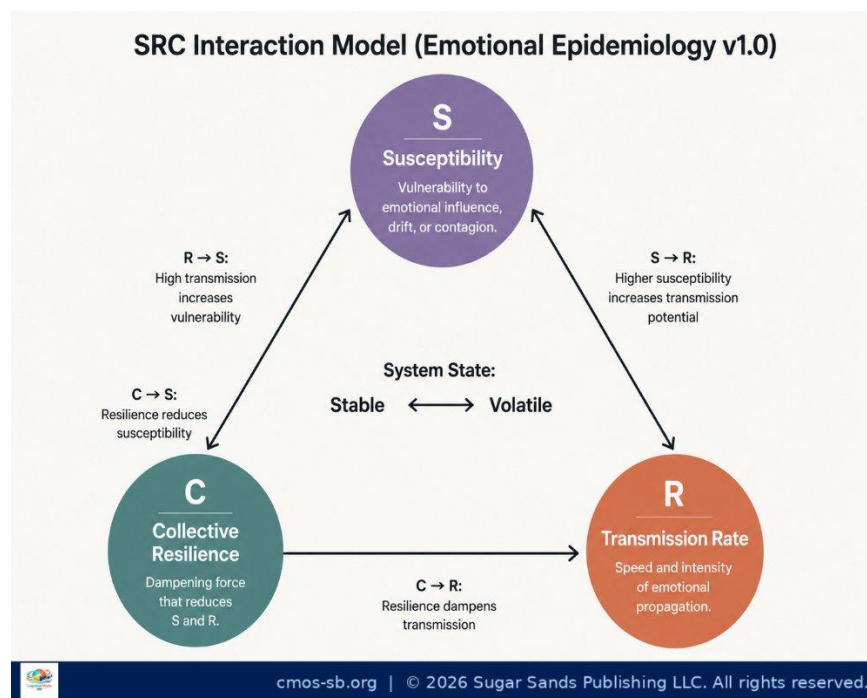


Figure 1. The S-R-C Interaction Model (Emotional Epidemiology v1.0) — the three governing forces of population-level emotional dynamics.

2.2 The S-R-C Model — A Population-Level Framework

The **S-R-C Model** is the theoretical framework at the core of Emotional Epidemiology. It describes the three governing forces of population-level emotional dynamics and their interactions. Understanding the S-R-C Model is prerequisite to understanding why CMOS-SB standards are structured the way they are and what system behaviors they are designed to prevent.

S — Susceptibility

Susceptibility refers to the degree of vulnerability a population or individual has to emotional influence, drift, or contagion. Susceptibility is not a fixed individual trait — it is a contextual, dynamic, systemic property. High susceptibility is produced by conditions including elevated stress load, relational instability, prior emotional exposure, system design choices that weaken user agency, and environmental conditions including noise, disruption, and uncertainty. Susceptibility is the primary

target of EISS and CMSS standards, both of which establish requirements designed to minimize system-generated susceptibility and protect users operating under conditions of pre-existing vulnerability.

R — Transmission Rate

Transmission Rate refers to the speed and intensity at which emotional states propagate through a population or network. High transmission is produced by platform design choices that maximize engagement velocity, interaction frequency, and emotional amplification; by network topologies that concentrate influence in high-reach nodes; and by content architectures that preferentially surface emotionally activating material. Transmission Rate is the primary target of ETDS and PERMS standards, which establish transparency requirements and population-level monitoring requirements designed to detect and mitigate high-transmission dynamics.

C — Collective Resilience

Collective Resilience is the dampening force that reduces both Susceptibility and Transmission Rate. It represents the system-level capacity to absorb emotional disruption, maintain relational stability, and recover from emotional events without cascading. Collective Resilience is built through relational trust, emotional safety design, recovery mechanisms, and the structural protections provided by CMOS-SB standards. It is the positive state that standards compliance is designed to build and sustain.

System State Dynamics

The S-R-C Model describes two characteristic system states: a **high-risk state** characterized by High S + High R + Low C, which produces cascading emotional contagion, drift, and potential mode collapse at the population level; and a **resilient state** characterized by Low S + Low R + High C, which produces a self-stabilizing system with high collective wellbeing and low vulnerability to emotional disruption. All CMOS-SB standards are oriented toward moving systems from the high-risk state toward the resilient state by reducing susceptibility, limiting transmission intensity, and building collective resilience through design requirements, transparency obligations, and population-level monitoring.

2.3 Cognitive Mode OS Theory — The Governing Layer

Cognitive Mode OS Theory is the governing layer of the CMOS-SB framework. It treats human cognition as a dynamic, state-based system with identifiable modes, predictable transitions, measurable baselines, definable constraints, observable failure modes, and recoverable states — analogous, in structural terms, to a technical operating system that can be described, monitored, and governed. This is an explicit and intentional parallel: just as an operating system manages computational resources, allocates processing capacity, and protects against overload, the cognitive mode system manages attentional resources, regulates emotional processing, and maintains the boundaries required for stable, functional operation.

Critically, Cognitive Mode OS Theory does not classify, profile, or diagnose individuals. It defines the system boundaries — the operating parameters — within which digital systems must function in order to interact safely with human cognition. A system that pushes users into cognitive overload, that fails to detect mode transitions, that amplifies emotional activation without safeguards, is not merely poorly designed — it is operating outside safe system boundaries. Cognitive Mode OS Theory provides the conceptual and technical vocabulary for defining those boundaries, monitoring compliance with them, and designing systems that respect them.

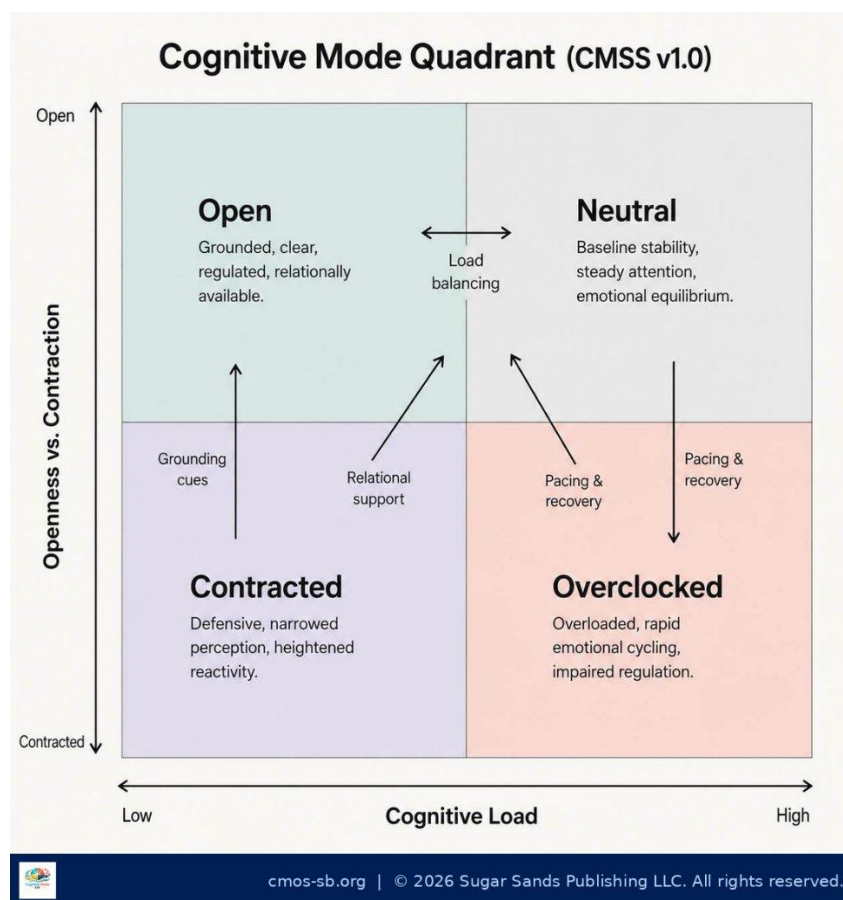


Figure 2. The Cognitive Mode Quadrant (CMSS v1.0) — four cognitive states mapped across Openness and Cognitive Load dimensions.

2.4 Zero Trust Evolution — The Cybersecurity Parallel

The evolution of **Zero Trust** in cybersecurity provides the clearest existing parallel to the CMOS-SB governance project and serves as both intellectual precursor and structural model. Zero Trust began as a simple behavioral heuristic — "Never Trust, Always Verify" — and evolved over successive maturity levels into a comprehensive, architecture-level security governance framework. The parallel to CMOS-SB is precise: emotional safety began as an individual concern and must now be elevated to an architecture-level governance framework for systems operating at scale.

The four maturity levels of Zero Trust evolution are as follows:

- **1.0 Basic Training:** Simple behavioral rules — Don't Click, Never Trust, No Sharing. Addressed individual behavior, not system architecture.

- **2.0 Enterprise Security:** Conditional Access, Device Compliance, Privilege Management. Introduced system-level controls but remained primarily perimeter-focused.
- **3.0 Identity as Architecture:** Adaptive Policies, Trust Contexts, Continuous Validation. Elevated identity to a first-class architectural element, enabling dynamic trust decisions.
- **3.5+ Cognitive Zero Trust:** Cognitive Permissions, Human + AI Signals, Emotional Security. The emerging maturity level at which the cognitive and emotional state of users becomes a first-class architectural consideration — the domain governed by CMOS-SB.



Figure 3. Zero Trust Evolution — from Basic Training to Cognitive Zero Trust at maturity level 3.5+.

PART III

The CMOS-SB Ecosystem

3.1 The Five-Line Architecture

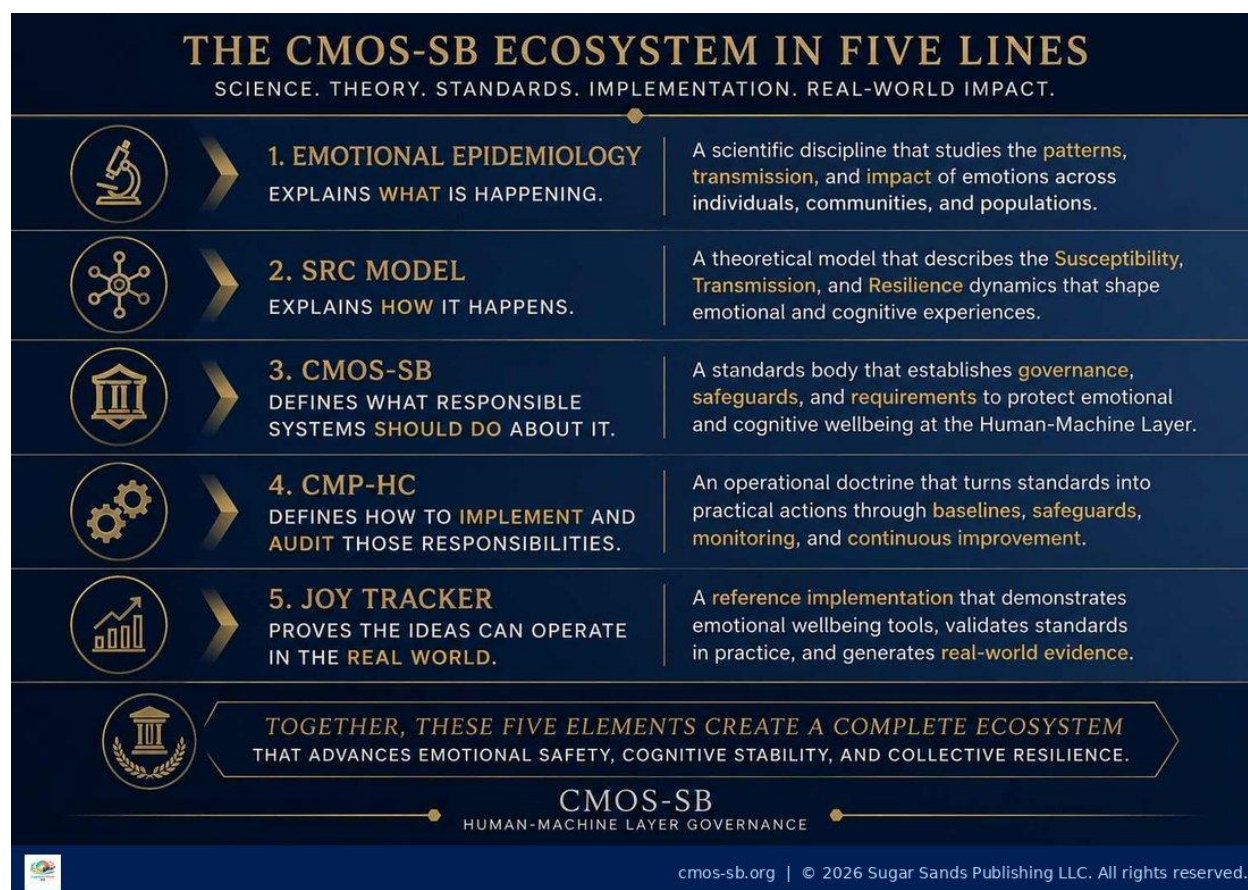


Figure 4. The CMOS-SB Ecosystem in Five Lines — Science. Theory. Standards. Implementation. Real-World Impact.

The CMOS-SB ecosystem is organized around five lines, each performing a distinct and necessary function. Together, they constitute the world's first complete framework for emotional infrastructure safety and cognitive mode governance. Each line depends on the others, and none is complete without the rest. The five lines are not sequential stages — they are simultaneous, interdependent, and mutually reinforcing dimensions of a single integrated ecosystem.

Line 1 — Emotional Epidemiology: Science. Explains WHAT IS HAPPENING.

Emotional Epidemiology is the scientific discipline that studies the patterns, transmission, and impact of emotions across individuals, communities, and populations. It provides the empirical and theoretical foundation upon which everything else rests. Without the science of Emotional Epidemiology, there is no principled basis for the standards, no evidence base for the governance requirements, and no credible claim that the framework addresses real and measurable phenomena. Emotional Epidemiology is the answer to the question: What is actually happening when digital systems interact with human emotional states at scale?

Line 2 — S-R-C Model: Theory. Explains HOW IT HAPPENS.

The S-R-C Model is the theoretical framework that translates the empirical findings of Emotional Epidemiology into a formal, operationalizable description of mechanism. It explains how emotional states propagate — through the interplay of Susceptibility, Transmission Rate, and Collective Resilience — and provides the conceptual vocabulary needed to design interventions, set governance requirements, and evaluate outcomes. Without the S-R-C Model, the science of Emotional Epidemiology has no governing mechanism; the standards have no theoretical grounding; and the safeguards have no principled design logic.

Line 3 — CMOS-SB: Standards. Defines WHAT RESPONSIBLE SYSTEMS SHOULD DO ABOUT IT.

CMOS-SB is the standards body that translates the science and theory of Emotional Epidemiology into governance requirements for systems operating at the Human-Machine Layer. It establishes what responsible systems must do — the safeguards they must implement, the transparency they must provide, the consent they must obtain, the monitoring they must conduct — to operate safely in the presence of human emotional vulnerability. CMOS-SB is the answer to the question: Given what we know about emotional dynamics and their risks, what obligations follow for system designers, operators, and deployers?

Line 4 — CMP-HC: Doctrine. Defines HOW TO IMPLEMENT AND AUDIT THOSE RESPONSIBILITIES.

The Configuration Management Plan for Human Cognition (CMP-HC) is the operational doctrine that turns CMOS-SB standards into practical, auditable, implementable actions. CMP-HC provides the control architecture, the compliance domains, the traceability schema, and the audit readiness framework that

organizations need to translate governance requirements into operational reality. Without CMP-HC, CMOS-SB standards remain aspirational; with CMP-HC, they become implementable.

Line 5 — Joy Tracker: Implementation. Proves THE IDEAS CAN OPERATE IN THE REAL WORLD.

Joy Tracker is the first operational application of Emotional Epidemiology and the reference implementation for CMOS-SB standards. It proves that the concepts, models, standards, and doctrines described in Lines 1 through 4 are not merely theoretical — that they can be built, deployed, and validated in real-world conditions, generating real evidence about emotional dynamics, real data supporting the scientific claims of Emotional Epidemiology, and real proof that emotional wellbeing tools built on CMOS-SB standards can function effectively and safely.

3.2 The Governance Spine — Five Standards Pillars



Figure 5. The CMOS-SB Governance Spine — five foundational standards pillars.

EISS — Emotional Infrastructure Safety Standard (CMOS-SB Standard 1001)

The Emotional Infrastructure Safety Standard (EISS) establishes the foundational safety requirements that any system interacting with human emotional states must meet. EISS defines baseline emotional safety obligations — including transparency about emotional inference capabilities, emotional-risk minimization requirements, relational integrity protections, and equity provisions ensuring that safety standards apply consistently across user populations without discriminatory gaps. EISS is the floor of the Governance Spine: all other standards build upon its baseline protections.

CMSS — Cognitive Mode Stability Standard (CMOS-SB Standard 1002)

The Cognitive Mode Stability Standard (CMSS) governs the management of cognitive states at the Human-Machine Layer. It establishes requirements for mode identification, transition safety, load balancing, drift detection, and recovery pathway implementation. CMSS prevents systems from pushing users into states of cognitive overload, contraction, or volatility by defining what safe system behavior looks like at each cognitive mode and what interventions are required when unsafe transitions or drift patterns are detected. CMSS operationalizes Cognitive Mode OS Theory as a governance requirement.

ETDS — Emotional Transparency & Disclosure Standard (CMOS-SB Standard 1003)

The Emotional Transparency and Disclosure Standard (ETDS) establishes mandatory disclosure requirements for systems that infer, respond to, or influence human emotional states. ETDS requires that users be clearly and accessibly informed about a system's emotional inference capabilities, its response mechanisms, the potential impacts of its emotional outputs, and the limitations of its emotional processing. The guiding principle of ETDS is unconditional: opaque emotional influence — influence that occurs without disclosure, without user awareness, and without meaningful consent — is prohibited. This is the transparency pillar of the Governance Spine.

EDCPS — Emotional Data Consent & Privacy Standard (CMOS-SB Standard 1004)

The Emotional Data Consent and Privacy Standard (EDCPS) establishes the consent, minimization, retention, and anti-surveillance requirements governing the collection, use, and storage of emotional data. EDCPS mandates explicit, informed consent for the collection of emotional signals; requires that data collection be minimized to what is necessary for stated purposes; establishes retention limits; prohibits use of emotional data for surveillance, manipulation, or unauthorized profiling; and guarantees data subject rights including the right to withdrawal and the right to deletion. EDCPS is the privacy and consent pillar of the Governance Spine.

PERMS — Population-Level Emotional Risk Monitoring Standard (CMOS-SB Standard 1005)

The Population-Level Emotional Risk Monitoring Standard (PERMS) establishes the monitoring, detection, and reporting requirements that enable systems to identify and respond to population-level emotional risk patterns before they reach crisis thresholds. PERMS defines baseline stability metrics, early warning indicators, high-risk thresholds, anomaly detection requirements, cluster mapping protocols, escalation pathways, and reporting obligations. PERMS applies the public health surveillance

model to digital emotional infrastructure, treating population-level emotional dynamics as a domain requiring systematic, ongoing monitoring — not reactive response after harm has occurred.

3.3 Reference Architecture RA-1.0

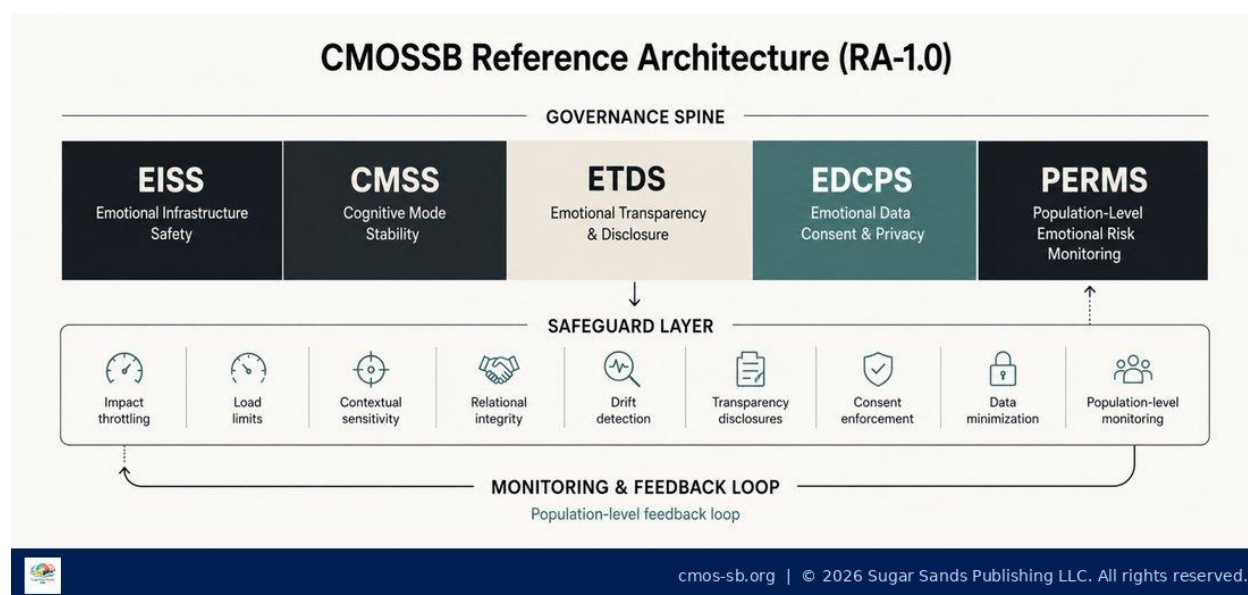


Figure 6. CMOS-SB Reference Architecture (RA-1.0) — Governance Spine, Safeguard Layer, and Monitoring & Feedback Loop.

The CMOS-SB Reference Architecture (RA-1.0) defines the three-layer structural model within which compliant systems must operate. It is the architectural translation of the Governance Spine into an implementable design pattern.

Layer 1 — Governance Spine

The Governance Spine is the normative foundation: the five published standards (EISS, CMSS, ETDS, EDCPS, PERMS) that define what safe behavior at the Human-Machine Layer looks like. The Governance Spine does not specify implementation architectures — it specifies outcomes and obligations. Any compliant system architecture must be demonstrably capable of meeting the requirements of all five standards simultaneously.

Layer 2 — Safeguard Layer

The Safeguard Layer is the operational implementation of Governance Spine requirements through specific technical and procedural controls. The Safeguard Layer includes: impact throttling (limiting the

rate and intensity of emotional signal delivery); load limits (preventing cognitive overload through concurrent task and complexity constraints); contextual sensitivity controls (modulating system behavior based on detected emotional context); relational integrity guardrails (ensuring tone, empathy, and boundary protections); drift detection mechanisms (identifying and correcting baseline deviations); transparency disclosures (surfacing required ETDS information at appropriate interaction points); consent enforcement (implementing EDCPS requirements at all emotional data collection points); data minimization controls (limiting collection to necessary data); and population-level monitoring (implementing PERMS surveillance and reporting requirements).

Layer 3 — Monitoring & Feedback Loop

The Monitoring and Feedback Loop is the continuous evaluation mechanism that enables the system to assess its own compliance performance, detect emerging risks, and generate evidence for governance review. The feedback loop operates at three levels: individual interaction monitoring (real-time safeguard performance); aggregate population monitoring (PERMS-aligned surveillance); and governance cycle integration (feeding findings back into standards revision, audit, and certification processes). The closed-loop nature of this architecture is a defining feature of RA-1.0: compliance is not a static state but a continuously validated condition.

PART IV

Standards Canon

4.1 EISS v1.0 — Emotional Infrastructure Safety Standard

CMOS-SB Standard 1001 | Effective: June 9, 2026 | Status: Active

Purpose

To establish baseline safety requirements for any system interacting with, influencing, or responding to human emotional states. EISS defines the minimum conditions of safety that must be met before deployment and maintained during operation. It is the foundational safety floor of the CMOS-SB Governance Spine.

Scope

EISS applies to: digital systems that infer, respond to, or influence emotional states; AI-enabled systems with adaptive response capabilities; platforms mediating emotional interactions at scale; tools that generate or modulate emotional signals; and environments designed to produce population-level emotional effects. EISS does **not** apply to: purely mechanical systems with no emotional inference or output capability; purely offline personal-use applications not deployed for third-party use; or artistic works not deployed as interactive systems capable of emotional inference.

Key Definitions

- **Emotional-Infrastructure System:** Any digital system that interacts with, influences, or responds to human emotional states or cognitive modes at any scale.
- **Emotional-Risk Transmission:** The propagation of emotional states, signals, or activations through a system or network in ways that may increase susceptibility, amplify distress, or accelerate drift in users or populations.
- **Cognitive Mode:** A discrete, identifiable state of human cognitive-emotional functioning characterized by distinct inputs, outputs, constraints, and transition conditions.
- **Population-Level Emotional Dynamics:** The aggregate patterns of emotional state, transmission, and stability observable across groups of users or defined populations.
- **Safeguard:** A technical or procedural control implemented to prevent, detect, or mitigate emotional or cognitive harm at the Human-Machine Layer.

Scientific Foundations

EISS is grounded in the findings of Emotional Epidemiology (Thompson, DOI: 10.5281/zenodo.20314466), which demonstrate that emotional states exhibit population-level transmission dynamics including susceptibility gradients, transmission rate variation, and collective resilience effects. The S-R-C Model provides the theoretical framework within which EISS requirements

are designed. Cognitive Mode OS Theory provides the operational framework within which EISS applies to individual user states.

Core Safety Requirements

5.1 Emotional Transparency: Systems must disclose, in clear and accessible language, (a) their capability to infer emotional states from user inputs or behaviors; (b) the mechanisms through which they respond to or modulate emotional signals; (c) the potential impacts of their emotional outputs on user states; and (d) the limitations of their emotional processing capabilities, including known error conditions and demographic variability.

5.2 Emotional-Risk Minimization: Systems must minimize unnecessary emotional intrusion into user states; avoid covert emotional influence — any modulation of user emotional states that occurs without user awareness or disclosure; prevent unnecessary activation of fear, distress, or high-arousal negative emotional states; avoid amplifying existing distress signals beyond what is necessary for the system's stated purpose; and implement safeguards proportionate to the assessed emotional-risk profile of the system's deployment context.

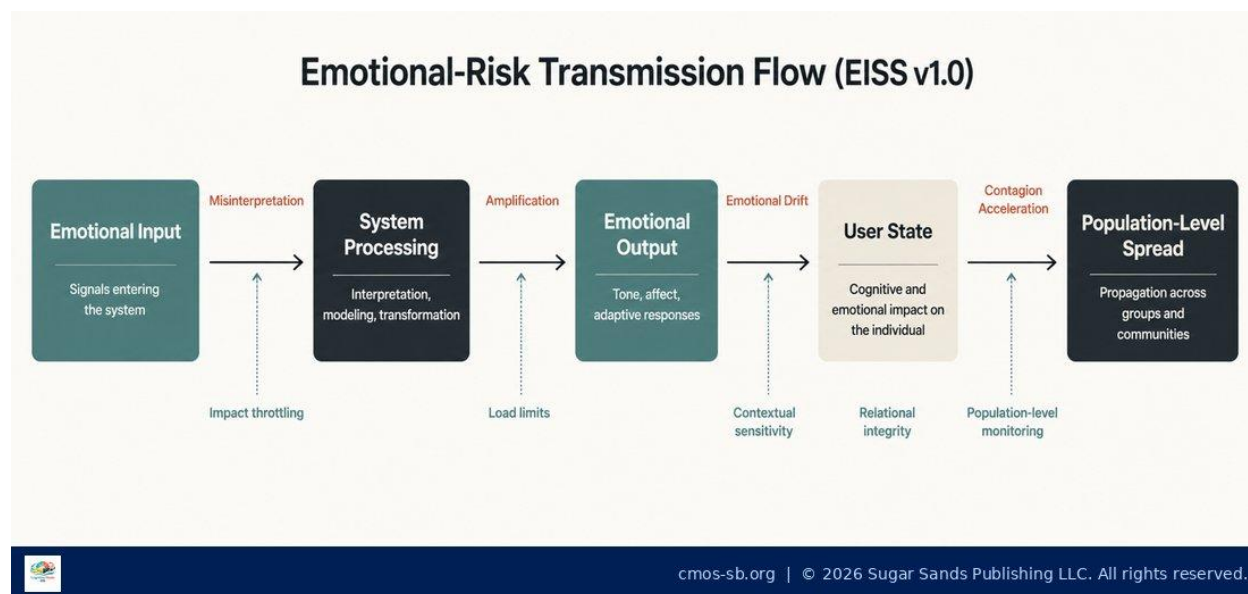


Figure 7. Emotional-Risk Transmission Flow (EISS v1.0) — five-stage propagation from Emotional Input to Population-Level Spread with safeguard feedback controls.

4.2 CMSS v1.0 — Cognitive Mode Stability Standard

CMOS-SB Standard 1002 | Effective: June 9, 2026 | Status: Active

The Cognitive Mode Stability Standard (CMSS) governs system behavior with respect to cognitive mode identification, transition safety, load balancing, drift detection, and recovery pathway implementation. CMSS defines four canonical cognitive states and establishes governance requirements for each.

The Four Cognitive States

Mode	Characteristics	System Requirements
Open	Grounded, clear, regulated, relationally available. Optimal state for learning, decision-making, and relational engagement.	Maintain conditions supporting Open state. Avoid unnecessary load introduction. Preserve relational safety.
Neutral	Baseline stability, steady attention, emotional equilibrium. Standard functional state for most interactions.	Monitor for drift indicators. Provide appropriate cognitive load management. Support transition to Open when indicated.
Contracted	Defensive, narrowed perception, heightened reactivity. Reduced openness to new information; increased error sensitivity.	Reduce load intensity. Activate grounding cues. Avoid high-complexity or high-stakes interactions. Initiate recovery pathway.
Overclocked	Overloaded, rapid emotional cycling, impaired regulation. High-risk state requiring immediate intervention.	Immediate load reduction. Activate pacing and recovery protocols. Suspend non-essential interactions. Escalate if sustained.

Transition Safety Rules

Mode transitions are the primary risk surface for cognitive destabilization. CMSS defines four transition types with associated governance requirements:

- **Load Balancing** (Open ↔ Neutral): Permitted as standard operation; must maintain load within defined parameters.
- **Grounding Cues** (Contracted → Open): System must detect Contracted state and activate appropriate grounding response before increasing interaction intensity.
- **Relational Support** (Contracted → Neutral): System must provide stabilizing relational signals before resuming standard interaction.

- **Pacing & Recovery** (Overclocked → Neutral or Contracted): System must immediately reduce pace and load; recovery must be treated as a system requirement, not a user responsibility.

Drift Detection and Load-Balancing Requirements

Systems must maintain continuous monitoring for indicators of mode drift — progressive movement away from stable baseline states. Drift detection must operate at both individual interaction level and aggregate population level (per PERMS requirements). Load balancing requirements establish maximum concurrent cognitive task loads, complexity metering protocols, and load-shedding procedures for conditions approaching overload thresholds. Recovery pathways must be defined, tested, and readily accessible for all deployed cognitive mode states.

4.3 ETDS v1.0 — Emotional Transparency & Disclosure Standard

CMOS-SB Standard 1003 | Effective: June 9, 2026 | Status: Active

The Emotional Transparency and Disclosure Standard (ETDS) establishes mandatory disclosure requirements for all systems within CMOS-SB scope. The foundational principle of ETDS is unconditional: **opaque emotional influence is prohibited without exception**. No system may modulate, infer, or respond to human emotional states without providing clear, accessible, and timely disclosure of that capability and its use.

Mandatory Disclosure Categories

- **Inference Disclosure:** Systems must disclose that they are capable of inferring emotional states from user inputs, and describe the types of signals used (e.g., text sentiment, behavioral patterns, interaction timing).
- **Adaptive Response Disclosure:** Systems must disclose that they adapt their responses based on inferred emotional states, and describe in accessible terms how that adaptation functions.
- **Impact Disclosure:** Systems must disclose the potential emotional impacts of their outputs, including known risks of amplification, activation of distress, or relational boundary effects.
- **Limitations Disclosure:** Systems must disclose the known limitations and error conditions of their emotional processing, including demographic variability in inference accuracy.

Timing and Format Requirements

Disclosures must be provided at or before first interaction with emotional inference capability; upon any material change to emotional processing functions; and upon user request at any time. Format requirements mandate plain language accessible to the general public without technical background; availability in all languages in which the system is deployed; and accessibility for users with visual, cognitive, or language disabilities.

4.4 EDCPS v1.0 — Emotional Data Consent & Privacy Standard

CMOS-SB Standard 1004 | Effective: June 9, 2026 | Status: Active

The Emotional Data Consent and Privacy Standard (EDCPS) governs the collection, use, retention, and protection of emotional data. Emotional data — any data derived from or used to infer human emotional states — is treated as a category of sensitive personal information requiring heightened protections beyond general data privacy requirements.

Consent Requirements

Explicit, informed consent is required before any collection of emotional data. Consent must be: specific to the purpose of collection; granular (users may consent to some emotional data uses while declining others); freely given without conditioning system access on consent to non-essential emotional data collection; and readily withdrawable at any time without penalty or degraded service for core system functions.

Data Minimization and Retention

Collection of emotional data must be minimized to what is demonstrably necessary for the stated purpose. Systems must establish and publish retention limits for all categories of emotional data. Data must be deleted upon user request, upon expiry of retention period, or upon withdrawal of consent, whichever occurs first.

Anti-Surveillance Protections

Emotional data may not be used for surveillance, behavioral manipulation, unauthorized profiling, or any purpose not disclosed to and consented to by the user. Cross-system sharing of emotional data is

prohibited except where explicitly consented and subject to equivalent protections in the receiving system. Data subject rights include: right of access, right to correction, right to deletion, right to portability, and right to object to processing.

4.5 PERMS v1.0 — Population-Level Emotional Risk Monitoring Standard

CMOS-SB Standard 1005 | Effective: June 9, 2026 | Status: Active

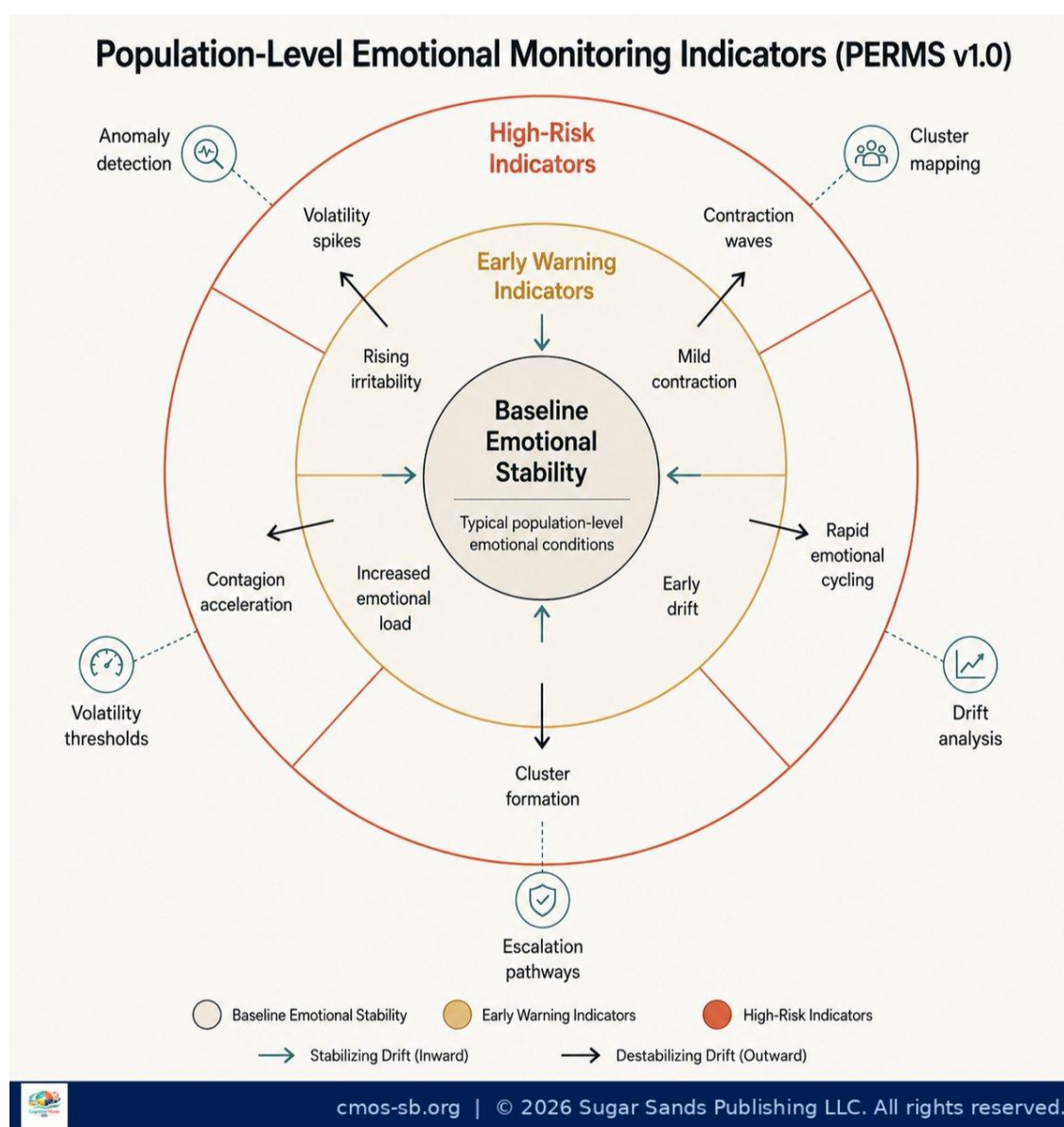


Figure 8. PERMS v1.0 Population-Level Emotional Monitoring Indicators — concentric-ring model from Baseline Stability through Early Warning to High-Risk Indicators.

The Population-Level Emotional Risk Monitoring Standard (PERMS) applies the principles of epidemiological surveillance to digital emotional infrastructure. It requires systems to monitor aggregate emotional state patterns across their user populations, detect early warning indicators, identify high-risk dynamics, and respond through defined escalation pathways.

Baseline Establishment

Systems must establish documented population-level emotional baselines against which anomalies, drift, and escalation can be measured. Baselines must be updated at defined intervals and upon material changes in system design or deployment context. Baseline data is subject to EDCPS protections; all monitoring must operate on anonymized and aggregated data.

Early Warning Indicators

- Rising irritability scores across user cohorts
- Mild contraction patterns in interaction data
- Increased emotional load signals across defined user segments
- Early drift indicators — progressive movement away from established baseline

High-Risk Indicator Definitions

- Volatility spikes — sudden, sharp increases in emotional activation variance
- Contraction waves — rapid propagation of contracted cognitive modes across user population
- Rapid emotional cycling — high-frequency mode transitions across cohorts
- Contagion acceleration — increasing transmission rate detected through interaction pattern analysis

Escalation Pathways and Reporting

Systems must define and document escalation pathways for early warning and high-risk indicators. Escalation must include: internal notification to responsible governance personnel; assessment and response within defined time windows; and external reporting for sustained high-risk conditions. Reporting requirements include periodic aggregate reports to CMOS-SB, incident reports upon confirmed high-risk events, and annual population-level monitoring summaries.

PART V

CMP-HC: Operational Doctrine

5.1 What CMP-HC Is

The **Configuration Management Plan for Human Cognition (CMP-HC)** is the world's first structured framework for understanding, stabilizing, and governing the cognitive and emotional interfaces between humans and intelligent systems. CMP-HC is the operational doctrine that translates CMOS-SB standards from governance requirements into implementable, auditable, traceable controls.

Foundational Distinction

CMP-HC is the doctrine. CMOS-SB is the standards body. CMP-HC tells organizations how to implement CMOS-SB standards in practice. CMOS-SB defines what responsible behavior looks like. Together, they constitute the complete operational and normative framework for Human-Machine Layer governance.

CMP-HC is emphatically **not** a product, a therapy model, or a behavioral framework. It is a systems-engineering discipline applied to the human cognitive-emotional architecture. It borrows the rigor, precision, and auditability of configuration management — a well-established domain in IT governance — and applies it to the novel challenge of governing the interface between digital systems and human cognition. The result is a framework that is simultaneously technically rigorous, clinically informed, governance-oriented, and practically implementable.

5.2 CMP-HC Technical Architecture — Six Primary Components

1. Cognitive Baseline

The cognitive baseline defines the stable operating range for a given deployment context, characterized by attentional bandwidth, emotional load tolerance, relational sensitivity, cognitive processing capacity, and environmental stress thresholds. Critically, baselines are contextual, not personal — they describe the expected operating parameters for a defined class of interaction context, not individual psychological profiles. Establishing an accurate cognitive baseline is the prerequisite for all subsequent mode identification, transition monitoring, and safeguard calibration.

2. Cognitive Modes

Cognitive modes are discrete, identifiable states of the human cognitive-emotional system, defined by their characteristic inputs, outputs, constraints, transition conditions, and failure conditions. CMP-HC operationalizes the four modes defined in CMSS (Open, Neutral, Contracted, Overclocked) as configurable system states against which monitoring and response logic can be calibrated. Mode identification is a system requirement; systems must have defined mechanisms for detecting mode signals and responding appropriately.

3. Mode Transitions

Mode transitions are the primary risk surface for cognitive destabilization. CMP-HC defines transition rules in terms of triggers, thresholds, hysteresis (the lag between a trigger condition and a transition response, preventing oscillation), stabilization requirements, and recovery pathways. Transition logic must be explicitly documented in system configuration, tested during deployment qualification, and monitored continuously during operation. Unauthorized or undetected transitions are compliance failures.

4. Emotional-Signal Interfaces

Emotional-signal interfaces are the technical points at which systems read emotional signals, modulate emotional load, influence cognitive state, or alter relational dynamics. CMP-HC requires that all emotional-signal interfaces be explicitly documented, subject to defined boundary controls that prevent overmodulation and emotional drift, and included in the system's audit surface. Interface boundaries are the implementation location of EISS and ETDS controls.

5. Risk Surfaces

Risk surfaces are the locations within a system's architecture where human-system interaction can produce cognitive destabilization, emotional overload, relational distortion, attentional collapse, or mode collapse. CMP-HC requires that risk surfaces be explicitly identified, documented, and mapped to safeguard controls during system design. Risk surface mapping is a required element of CMP-HC audit documentation.

6. Recovery Pathways

Recovery pathways are the structured processes through which users return to stable cognitive baselines following a mode transition, overload event, or drift episode. CMP-HC establishes the principle — grounded in both human factors engineering and the S-R-C Model — that recovery is a system requirement, not a user responsibility. Systems must define, implement, test, and document recovery pathways for all identified risk surfaces. Recovery must be accessible, non-stigmatizing, and proportionate to the severity of the precipitating event.

5.3 CMP-HC Compliance Domains — Six Domains

Domain	Abbreviation	Scope
Access & Identity Management	AIM	Controls governing who may interact with emotional systems, under what conditions, and with what permissions.
Data Protection & Privacy	DPP	Controls implementing EDCPS requirements: consent, minimization, retention, anti-surveillance, and data subject rights.
Change & Configuration Management	CCM	Controls governing changes to system configuration that may affect cognitive mode behavior, emotional signal processing, or safeguard function.
Security Operations & Incident Management	SOIM	Controls governing detection, response, and recovery for emotional safety incidents, including mode collapse events and contagion episodes.
Business Continuity & Disaster Recovery	BCDR	Controls ensuring that emotional safety protections are maintained during system disruptions, failover events, and recovery operations.

Domain	Abbreviation	Scope
Regulatory Compliance & Audit Readiness	RCAR	Controls ensuring that systems are continuously audit-ready against applicable regulatory and CMOS-SB governance requirements.

Traceability Schema Domains

The CMP-HC Traceability Schema organizes evidence across six domains: **Cognitive-Mode Safety (CMS)**, **Telemetry Integrity (TI)**, **Governance Controls (GC)**, **Equity & Access (EA)**, **Operational Readiness (OR)**, and **Adversarial Safety & Pen Testing (AS)**.

Regulatory Scope

CMP-HC is designed to support compliance across the following regulatory frameworks: HIPAA, HITECH, 21 CFR Part 11, NIST SP 800-53, SOC 2 Type II, Centers for Medicare & Medicaid Services (CMS) Conditions of Participation (CoP), Joint Commission standards, and HITRUST CSF.

5.4 Control Architecture — Sample Control Mappings

Control ID	Control Name	CMP-HC Domain	CMOS-SB Category	Governance ID
CMP-HC-MD-01	Mode Identification – Baseline Detection	MD	Operational Controls	CMOS-SB-OP-01
CMP-HC-MD-02	Mode Display – User-Facing Verification	MD	User Protection	CMOS-SB-UP-02
CMP-HC-MD-03	Mode Transition Logging Integrity	MD	Information Governance	CMOS-SB-IG-06
CMP-HC-MD-04	Mode Transition Safety Rules	MD	Operational Controls	CMOS-SB-OP-04
CMP-HC-WF-01	Workflow Safety Check – Pre-Action Verification	WF	Operational Controls	CMOS-SB-OP-05

5.5 CMP-HC ↔ CMOS-SB Translation Matrix

CMP-HC Domain	CMOS-SB Domain	Relationship	Notes
Clinical Mode Safety	Oversight & Accountability	Direct	Governance adds escalation and reporting requirements
Human Factors & Workflow	Operational Controls	Direct	Governance adds evidence rigor and audit trail requirements
Emotional Epidemiology	Risk & Impact Assessment	Conceptual	Governance reframes population dynamics as formal risk categories
Patient Interaction Safety	User Protection Controls	Direct	Governance adds severity classification and auditability requirements
Data Handling & Boundaries	Information Governance	Direct	Governance adds traceability schema and retention controls
Organizational Culture	Governance & Leadership	Partial	Governance formalizes expectations that culture treats as implicit

PART VI

Safeguard Implementation

6.1 Safeguard Design Pattern Set (CMOS-SB v1.0)

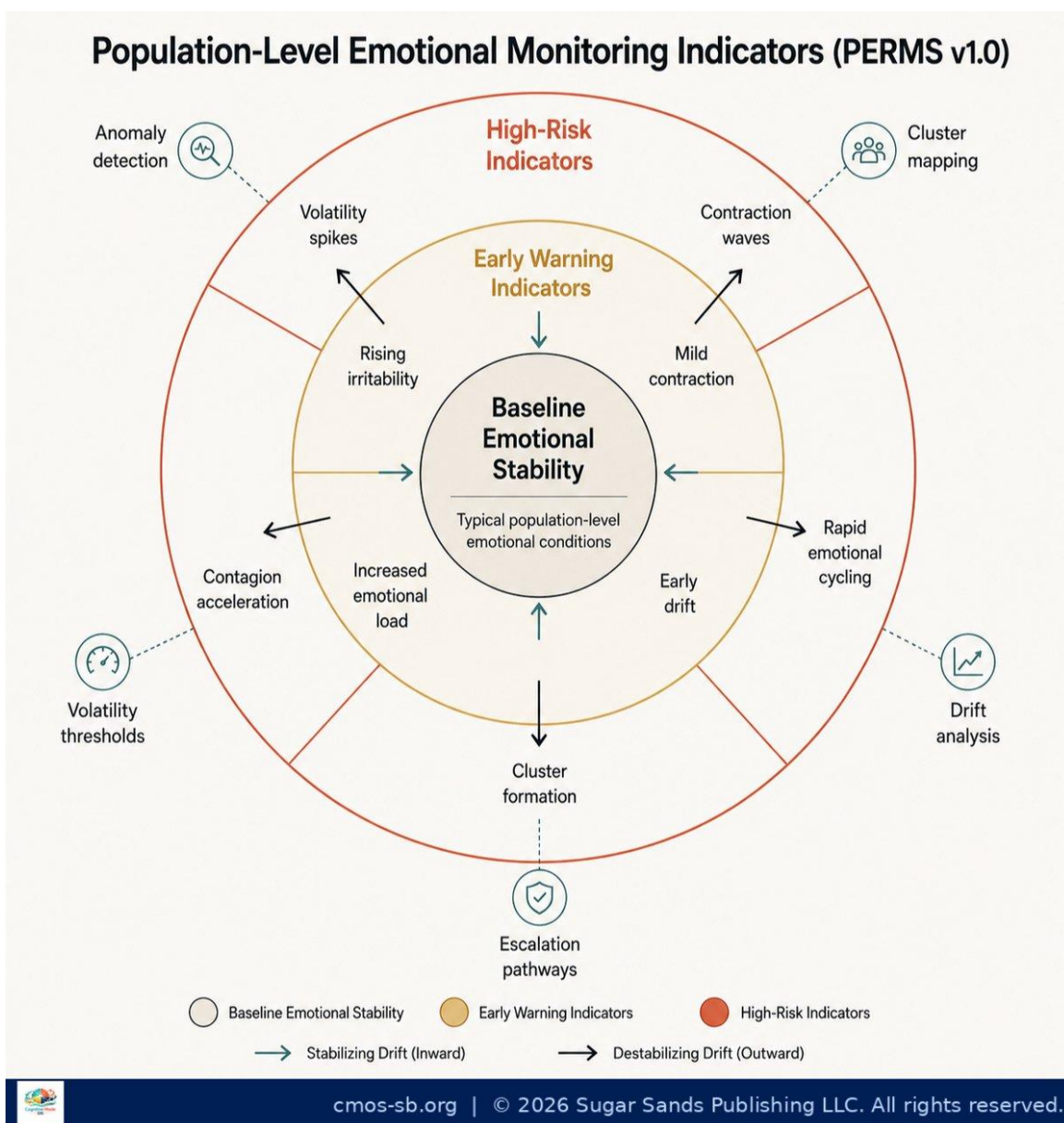


Figure 9. Safeguard Design Pattern Set (CMOS-SB v1.0) — six operational design patterns for emotional and cognitive safety.

The CMOS-SB Safeguard Design Pattern Set defines six operational design patterns that provide implementable, reusable solutions to the most common emotional and cognitive safety challenges at the Human-Machine Layer. Each pattern describes a problem domain, a design solution, and specific implementation requirements.

Pattern 1 — Emotional-Impact Throttling

Flow: Input → Throttle → Output

Emotional-Impact Throttling prevents sudden spikes in emotional intensity that could trigger mode transitions, amplify susceptibility, or accelerate transmission. The throttle acts as a rate-limiting and intensity-capping control on emotional signal delivery. Implementation requirements include: rate limiting on emotional signal delivery within defined interaction windows; intensity caps preventing activation levels from exceeding defined thresholds per interaction unit; and escalation detection triggers that activate additional safeguards when intensity approaches threshold limits. This pattern directly implements EISS 5.2 (Emotional-Risk Minimization) and CMSS load management requirements.

Pattern 2 — Cognitive-Load Balancing

Flow: Input → Load Balancer → Regulated Output

Cognitive-Load Balancing prevents overload states by distributing cognitive demand across time and interaction space, ensuring that no interaction window exceeds the cognitive load capacity of the target user context. Implementation requirements include: concurrent task limits establishing maximum simultaneous cognitive demands; complexity metering measuring and limiting the processing demand of individual interactions; and load-shedding protocols that automatically reduce complexity and pace when load approaches defined thresholds. This pattern implements CMSS mode transition safety rules and Overclocked-state intervention requirements.

Pattern 3 — Contextual Sensitivity Filter

Flow: Input → Context Filter → Interpretation

The Contextual Sensitivity Filter reduces emotional misinterpretation and drift by ensuring that system responses are calibrated to the detected emotional context rather than applied uniformly regardless of state. This is particularly important in systems serving diverse user populations with different baseline emotional contexts, cultural frameworks, and interaction histories. Implementation requirements include: context-aware parsing that detects emotional context signals before interpreting user inputs; situational modulation that adjusts response parameters based on detected context; and cultural sensitivity parameters that account for demographic and cultural variability in emotional expression and interpretation. This pattern implements ETDS disclosure requirements and EISS equity provisions.

Pattern 4 — Relational Integrity Guardrail

Flow: Interaction → Guardrail → Safe Relational Output

The Relational Integrity Guardrail ensures that system interactions maintain appropriate tone, empathic calibration, and relational boundaries — preventing the formation of unhealthy relational dependencies, the erosion of appropriate human-machine boundaries, and the amplification of relational distress. Implementation requirements include: tone calibration ensuring system outputs maintain consistent, non-manipulative relational quality; dependency prevention detecting and interrupting patterns that suggest unhealthy relational attachment; and relational boundary enforcement maintaining the clearly disclosed nature of the human-machine relationship. This pattern implements EISS relational integrity provisions and ETDS adaptive response disclosure requirements.

Pattern 5 — Drift Detection & Correction Loop

Flow: Output → Drift Monitor → Correction → Output

The Drift Detection and Correction Loop provides continuous monitoring for emotional or cognitive drift — progressive, often gradual movement away from established baselines — and activates correction pathways before drift reaches threshold levels. This closed-loop design ensures that drift is caught and corrected before it produces mode transitions, overload, or population-level contagion. Implementation requirements include: baseline deviation detection measuring current output against established emotional and cognitive baselines; correction pathway activation triggering defined intervention responses when deviation exceeds specified thresholds; and loop monitoring ensuring that correction pathways are themselves functioning correctly and are not introducing additional instability. This pattern implements CMSS drift detection mandates and PERMS early warning requirements.

Pattern 6 — Population-Level Anomaly Detection

Flow: Many User States → Pattern Detector → Alerts

Population-Level Anomaly Detection aggregates individual user state signals to identify system-level emotional dynamics that are not visible at the individual interaction level — including susceptibility spikes, transmission acceleration, contagion wave formation, and collective mode collapse. This pattern implements the epidemiological surveillance function required by PERMS. Implementation requirements include: cross-user state aggregation combining individual emotional state signals into population-level indicators while maintaining EDCPS privacy protections through anonymization and aggregation; contagion pattern recognition identifying the characteristic signatures of emotional contagion dynamics;

and escalation alert thresholds triggering defined response protocols when population-level indicators reach early warning or high-risk levels.

6.2 Closed-Loop Control Effectiveness System

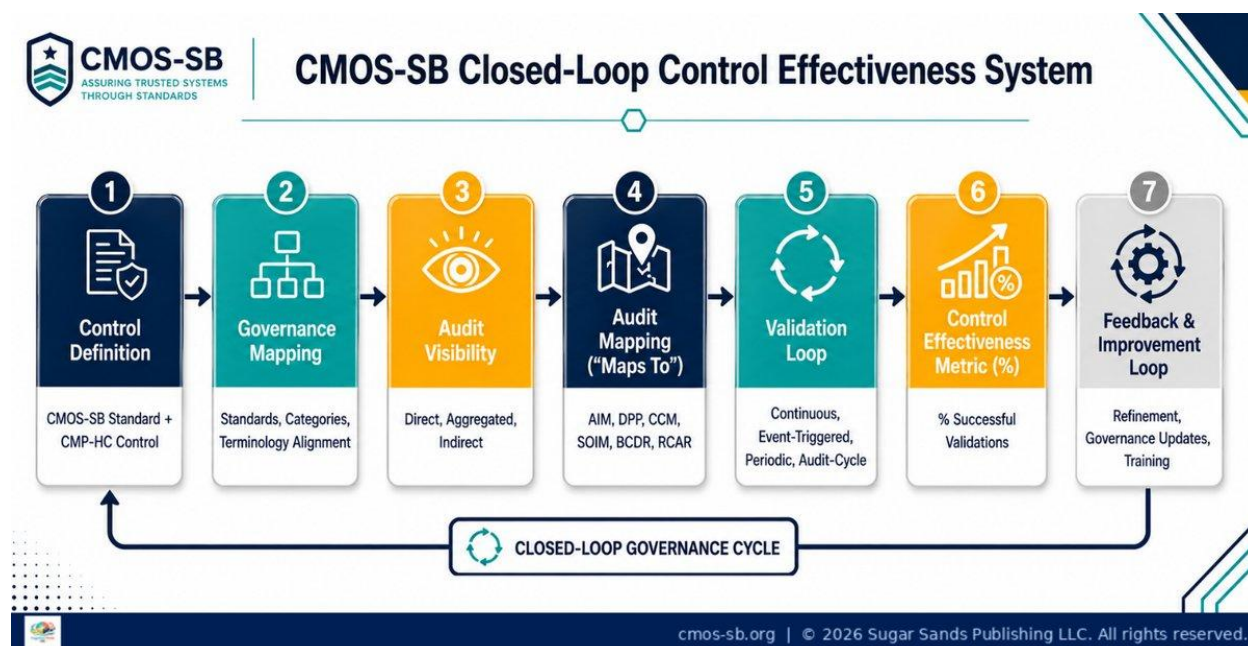


Figure 10. CMOS-SB Closed-Loop Control Effectiveness System — seven-step governance cycle ensuring continuous validation and improvement.

The CMOS-SB Closed-Loop Control Effectiveness System is the governance mechanism that ensures controls are not merely defined and deployed but continuously validated, measured, and improved. It transforms compliance from a point-in-time certification event into an ongoing operational practice.

Step 1 — Control Definition

Each control is defined with a CMOS-SB Standard reference, a control objective, a defined scope, and specific evidence requirements. Control definitions are documented in the CMP-HC control registry and versioned in alignment with the standards they implement. Control definitions must be sufficient for an independent auditor to assess compliance without additional clarification.

Step 2 — Governance Mapping

Each control is mapped to a CMOS-SB governance category, assigned a severity level (Critical, High, Medium, Low), and cross-referenced to applicable regulatory frameworks. Governance mapping ensures

that the organizational significance and regulatory relevance of each control are legible to governance, compliance, and audit functions.

Step 3 — Audit Visibility

Controls are assigned one of three audit visibility modes: **Direct** (control performance is directly observable in audit evidence); **Aggregated** (control performance is observable through aggregated metrics or logs); or **Indirect** (control performance is inferred from proxy indicators or process evidence). Visibility mode determines the evidence collection and audit methodology for each control.

Step 4 — Audit Mapping

Each control is mapped to one or more CMP-HC audit domains (AIM, DPP, CCM, SOIM, BCDR, RCAR), ensuring full traceability between controls and the compliance domains they support. Audit mapping enables gap analysis, domain-level compliance scoring, and regulatory cross-reference reporting.

Step 5 — Validation Loop

Controls are validated through four modes, each with defined triggers and frequencies: **Continuous** (automated, real-time monitoring for applicable controls); **Event-Triggered** (validation upon defined trigger events such as incidents, changes, or anomalies); **Periodic** (scheduled validation at defined intervals); and **Audit-Cycle** (comprehensive validation during formal audit periods). Validation mode is assigned based on control criticality and technical feasibility.

Step 6 — Control Effectiveness Metric

Each control is assigned a Control Effectiveness Metric (CEM) — a percentage representing the proportion of validation events in which the control performed as required. CEMs are calculated per control, per domain, and at aggregate program level. CEM thresholds are defined for each severity level: Critical controls require CEM $\geq 98\%$; High controls require CEM $\geq 95\%$; Medium controls require CEM $\geq 90\%$; Low controls require CEM $\geq 85\%$. Controls falling below threshold trigger defined remediation pathways.

Step 7 — Feedback & Improvement Loop

Control effectiveness findings feed back into the governance system through three pathways:

Refinement (adjustments to control design or implementation to improve performance); **Governance Updates** (escalation of systemic findings to standards revision processes through the Standards

Development Process); and **Training** (organizational learning programs addressing identified capability gaps). The feedback loop closes the governance cycle, ensuring that real-world operational performance continuously informs standards evolution.

PART VII

Governance Structure

7.1 Founding Charter — Constitutional Framework

The CMOS-SB Founding Charter is the constitutional foundation upon which all CMOS-SB standards, processes, and governance mechanisms are built. It is the authoritative statement of what CMOS-SB is, what it is authorized to do, how it is structured, and what principles govern its operation. The Charter cannot be amended except through a supermajority vote of the Board of Directors following a mandatory public consultation period.

The Charter serves five purposes:

1. Define the mission, authority, and jurisdictional scope of CMOS-SB
2. Establish the governance structure and the powers, responsibilities, and limitations of each governance body
3. Articulate the public-interest obligations that CMOS-SB assumes as a condition of its authority
4. Protect the independence of CMOS-SB from commercial, political, and institutional capture
5. Ensure that all standards-making processes are transparent, ethical, scientifically grounded, and publicly accountable

7.2 Governance Architecture — Multi-Body Structure

Board of Directors

The Board of Directors holds ultimate governance authority over CMOS-SB. It provides strategic oversight, ratifies standards following Committee approval, ensures organizational integrity, and holds the Standards Steward accountable for conceptual continuity. The Board must include a majority of members who are independent of any commercial entity that could benefit from CMOS-SB standards decisions. No single commercial entity may hold a majority of Board seats or fund more than 25% of CMOS-SB operating budget.

Standards Committee

The Standards Committee is the primary technical governance body responsible for standards development, review, revision, and initial approval. The Committee convenes expert panels, manages the Standards Development Process, administers the public comment process, and prepares standards for Board ratification. Committee membership requires demonstrated domain expertise and is subject to conflict-of-interest review.

Audit & Compliance Committee

The Audit and Compliance Committee oversees the integrity of the certification process, maintains the Compliance Registry, reviews and publishes interpretive rulings, and monitors post-publication implementation. It reports directly to the Board and operates independently of the Standards Committee to ensure separation of standard-setting and compliance-assessment functions.

Public Comment & Community Review Process

A mandatory 60-day public comment period is required for all new standards, all major revisions (MAJOR version increments), and all significant changes to governance structure. Public comments are received, documented, and formally responded to. Response to public comments is published as part of the standards publication record. This is not optional: public comment is a constitutional requirement of the CMOS-SB governance process.

Expert Panels and Working Groups

The Standards Committee may convene time-limited Expert Panels and Working Groups to provide specialized expertise for specific standards development tasks. Expert Panels include external subject matter experts from relevant disciplines including cognitive science, AI safety, public health, human factors engineering, legal and regulatory affairs, and community advocacy. Working Groups may include organizational stakeholders with relevant implementation experience.

7.3 Standards Development Process (SDP)

The CMOS-SB Standards Development Process (SDP) defines the required sequence for developing, reviewing, approving, and publishing standards. All standards must complete each stage in sequence; no stage may be bypassed.

Stage	Activity	Responsible Body
1. Proposal	Formal proposal submitted identifying need, scope, and scientific basis	Any stakeholder; received by Standards Committee
2. Scoping	Scope, applicability, and development timeline defined	Standards Committee
3. Draft Development	Standard drafted with expert panel input and scientific review	Standards Committee + Expert Panel
4. Internal Review	Standards Committee reviews and approves draft for public comment	Standards Committee
5. Public Comment (60 days)	Mandatory 60-day public comment period; comments documented	CMOS-SB Governance Office
6. Revision & Response	Draft revised; responses to public comments prepared and published	Standards Committee
7. Committee Vote	Final draft approved by Standards Committee	Standards Committee
8. Board Ratification	Board of Directors ratifies approved standard	Board of Directors
9. Publication	Standard published in Standards Registry with full publication record	CMOS-SB Governance Office
10. Post-Publication Monitoring	Implementation monitoring; findings reported; revision triggered if needed	Audit & Compliance Committee

Semantic Versioning

CMOS-SB standards use semantic versioning in the format MAJOR.MINOR.PATCH. MAJOR increments indicate breaking changes requiring full SDP including public comment. MINOR increments indicate non-breaking additions or clarifications requiring internal review and abbreviated public comment. PATCH increments indicate corrections or typographical fixes requiring Committee approval only.

7.4 Independence Protections

The independence of CMOS-SB from commercial, political, and institutional influence is a constitutional requirement, not an organizational preference. Independence protections include:

- **Conflict-of-Interest Policy:** All Board members, Committee members, and Expert Panel participants must disclose all relevant financial, organizational, and relational interests. Undisclosed conflicts are grounds for removal.
- **Recusal Requirements:** Members with identified conflicts must recuse from relevant votes and deliberations. Recusal is mandatory, not discretionary.
- **Transparent Decision Records:** All votes, deliberations (summary), and rationales for governance decisions are documented and made publicly available within defined timeframes.
- **Public Accountability Mechanisms:** CMOS-SB publishes annual governance reports, public comment response records, and compliance monitoring findings.
- **Hosting Entity Separation:** Sugar Sands Publishing LLC, as hosting entity, has no voting role in any CMOS-SB governance body. No employee or officer of SSP may simultaneously hold a governance role that creates a conflict with hosting responsibilities.
- **Funding Diversification Requirement:** No single commercial entity may fund more than 25% of CMOS-SB operating budget in any calendar year. Funding sources are publicly disclosed.

7.5 Certification and Compliance Registry

CMOS-SB maintains four public registries as part of its transparency and accountability obligations:

- **Standards Registry:** All published CMOS-SB standards with complete version history, publication records, public comment summaries, and interpretive rulings.
- **Certification Registry:** Organizations that have engaged the CMOS-SB certification process, with certification status, applicable standards, and certification dates.
- **Interpretive Rulings Registry:** Formal clarifications issued by the Audit and Compliance Committee in response to questions about standards interpretation. Interpretive rulings are binding on certification assessments.
- **Compliance Registry:** Aggregate compliance status information for certified organizations, published in a form that protects commercially sensitive details while enabling public accountability.

PART VIII

Regulatory and Cross-Framework Alignment

8.1 Regulatory Coverage Map

Regulatory Framework	CMP-HC Domain	CMOS-SB Standard	Relevance Notes
HIPAA	DPP, AIM, RCAR	EDCPS, EISS	Emotional data as protected health information (PHI) in clinical contexts; safeguard provisions align with Administrative, Physical, and Technical Safeguard requirements.

Regulatory Framework	CMP-HC Domain	CMOS-SB Standard	Relevance Notes
HITECH	DPP, SOIM, RCAR	EDCPS, PERMS	Breach notification requirements; enhanced enforcement provisions; audit log requirements align with PERMS monitoring mandates.
21 CFR Part 11	CCM, RCAR	ETDS, EISS	Electronic records and signatures requirements applicable to emotional data collection and audit trail integrity.
NIST SP 800-53	AIM, CCM, SOIM, RCAR	All	Broad control family alignment; CMOS-SB controls map to AC, AU, CM, IR, RA, and SC control families.
SOC 2 Type II	AIM, DPP, SOIM, BCDR	EISS, ETDS, EDCPS	Trust Services Criteria alignment across Security, Availability, Processing Integrity, Confidentiality, and Privacy.
CMS Conditions of Participation	AIM, DPP, SOIM	EISS, CMSS, EDCPS	Patient rights and quality standards applicable to digital health applications interacting with patient emotional states.
Joint Commission	SOIM, RCAR	CMSS, PERMS	Patient safety and quality standards; incident reporting requirements align with PERMS escalation pathways.
HITRUST CSF	All	All	Comprehensive risk management framework; CMOS-SB controls extend HITRUST CSF into the emotional and cognitive safety domain.

8.2 NIST SP 800-53 Alignment

CMOS-SB and CMP-HC controls align with the following National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 control families:

NIST Control Family	Abbreviation	CMOS-SB Alignment
Access Control	AC	AIM domain controls; EDCPS consent and access management requirements
Audit and Accountability	AU	CMP-HC MD-03 (Transition Logging Integrity); PERMS monitoring and reporting; closed-loop audit trail requirements

NIST Control Family	Abbreviation	CMOS-SB Alignment
Configuration Management	CM	CCM domain controls; emotional signal interface configuration; mode transition logic versioning
Incident Response	IR	SOIM domain controls; PERMS escalation pathways; emotional safety incident response protocols
Risk Assessment	RA	S-R-C Model risk assessment methodology; EISS risk-surface mapping; population-level risk monitoring (PERMS)
System and Communications Protection	SC	Emotional data transmission protections; anti-surveillance controls (EDCPS); cross-system sharing restrictions

8.3 SOC 2 Type II Alignment

SOC 2 Trust Services Criterion	CMOS-SB Standard(s)	CMP-HC Domain(s)	Alignment Notes
Security	EISS, EDCPS	AIM, SOIM	Emotional data access controls; security incident response; anti-surveillance protections
Availability	EISS, CMSS	BCDR	Safeguard availability during system disruptions; recovery pathway availability requirements
Processing Integrity	CMSS, ETDS	CCM, RCAR	Accuracy and completeness of emotional inference processing; disclosure integrity requirements
Confidentiality	EDCPS	DPP	Emotional data confidentiality; minimization; cross-system sharing restrictions
Privacy	EDCPS, ETDS	DPP, RCAR	Consent management; data subject rights; purpose limitation; retention controls

8.4 HIPAA/HITECH Alignment

HIPAA/HITECH Requirement Area	CMOS-SB Standard(s)	CMP-HC Domain(s)	Alignment Notes
Administrative Safeguards	EDCPS, EISS	AIM, RCAR	Risk analysis; workforce training; contingency planning; assigned security responsibility
Physical Safeguards	EDCPS	AIM	Facility access controls for systems processing emotional data in clinical environments
Technical Safeguards	EDCPS, ETDS	DPP, CCM	Access controls; audit controls; integrity protections; transmission security for emotional data
Breach Notification	EDCPS, PERMS	SOIM, RCAR	Emotional data breach notification requirements; PERMS escalation pathways as triggering mechanism

PART IX

Joy Tracker: Reference Implementation

9.1 Purpose and Role

Joy Tracker is the first operational application of Emotional Epidemiology and the designated reference implementation for CMOS-SB standards. Its role within the CMOS-SB ecosystem is foundational: it is the existence proof that the frameworks, standards, and doctrines described in this document are not merely theoretical constructs but functional realities that can be built, deployed, and validated in the world as it actually operates.

Joy Tracker demonstrates three things simultaneously. First, that emotional wellbeing tools can be built — that it is technically feasible to create digital applications that interact with human emotional states in ways that are safe, transparent, consent-based, and governed by CMOS-SB standards. Second, that CMOS-SB standards can be validated in practice — that the governance requirements defined in the

Governance Spine translate into implementable design choices and auditable controls. Third, that real-world evidence can be generated — that data produced by compliant emotional wellbeing tools contributes meaningfully to the scientific understanding of Emotional Epidemiology and the S-R-C Model dynamics it describes.

9.2 How Joy Tracker Validates the Ecosystem

Joy Tracker simultaneously serves as evidence base, proof of concept, test bed, real-world implementation, and feedback generator for each of the five ecosystem lines:

Ecosystem Line	Joy Tracker's Validation Role
Emotional Epidemiology (Science)	Generates empirical data demonstrating emotional state patterns, transmission dynamics, and population-level behaviors predicted by Emotional Epidemiology theory.
S-R-C Model (Theory)	Provides real-world evidence of Susceptibility, Transmission Rate, and Collective Resilience dynamics as they operate in deployed digital environments.
CMOS-SB (Standards)	Tests CMOS-SB Governance Spine standards against real deployment conditions, identifying implementation challenges and validating governance requirements.
CMP-HC (Doctrine)	Implements CMP-HC controls in a real operational context, demonstrating how doctrine translates into auditable system behavior.
Joy Tracker (Implementation)	Generates continuous feedback — operational findings, user experience data, compliance evidence — that flows back to improve all four preceding ecosystem lines.

9.3 Lessons from the Field

The development of Joy Tracker has been guided by the long-horizon field observation methodology described in the Emotional Epidemiology preprint (Thompson, I.A., 2026; DOI: 10.5281/zenodo.20314466). This methodology — grounded in extended observation of emotional state

patterns, contextual documentation, and systematic analysis of emotional dynamics over sustained time periods — provides the empirical substrate for the scientific claims of Emotional Epidemiology.

Joy Tracker generates digital emotional reporting data that demonstrates, in operational context, the three central findings of Emotional Epidemiology: that emotional states follow predictable spread patterns observable across users and over time; that emotional states respond systematically to environmental and network conditions in ways that are consistent with the S-R-C Model's predictions; and that emotional states exhibit measurable system-level behaviors — including drift patterns, transmission events, and collective resilience dynamics — that require governance at the system level rather than management at the individual level alone.

These field observations are not merely confirmatory of pre-existing theory. They are generative — continuously producing new insights about the mechanisms of emotional transmission, the conditions of collective resilience, and the design choices that most effectively protect against susceptibility and drift. This generative capacity is what makes Joy Tracker not merely a product but a scientific instrument and a governance laboratory — the living interface between the CMOS-SB framework and the world it was built to govern.

PART X

Implementation Roadmap

10.1 For Organizations Seeking Compliance

Organizations seeking to implement CMOS-SB standards should follow this structured six-step pathway. Each step builds on the previous; steps should not be reordered or collapsed.

6. Baseline Assessment against CMP-HC Domains

Conduct a comprehensive assessment of current organizational capabilities against the six CMP-HC compliance domains (AIM, DPP, CCM, SOIM, BCDR, RCAR). Document current state, capability gaps, and existing controls. The baseline assessment provides the factual foundation for all subsequent implementation planning.

7. Gap Analysis against CMOS-SB Governance Spine

Map current capabilities against the requirements of all five Governance Spine standards (EISS, CMSS, ETDS, EDCPS, PERMS). Identify specific gaps between current state and each standard's requirements. Prioritize gaps by severity, regulatory significance, and implementation complexity.

8. Safeguard Implementation using the Design Pattern Set

Use the CMOS-SB Safeguard Design Pattern Set to implement technical and procedural controls addressing identified gaps. Pattern selection should be based on the specific risk surfaces, cognitive mode dynamics, and population characteristics of the organization's deployment context. Document all safeguard implementations with reference to the controls they implement.

9. Closed-Loop Control Deployment

Deploy the Closed-Loop Control Effectiveness System across all implemented controls. Define validation modes, assign Control Effectiveness Metric (CEM) thresholds, establish monitoring cadences, and configure escalation pathways. Verify that the feedback loop is functional before proceeding to audit readiness.

10. Audit Readiness Preparation

Compile the evidence portfolio required for CMOS-SB certification assessment. Evidence must address all six Traceability Schema domains (CMS, TI, GC, EA, OR, AS) and demonstrate continuous control operation over a defined assessment period. Conduct internal pre-audit assessment against the CMP-HC Traceability Schema before engaging external assessment.

11. Certification Engagement

Engage the CMOS-SB Audit and Compliance Committee for formal certification assessment.

Provide evidence portfolio, baseline assessment documentation, and gap analysis. Certification findings are published in the Compliance Registry. Certification must be renewed annually and upon any MAJOR change to applicable standards.

10.2 For Standards Bodies and Regulators

CMOS-SB standards are designed for adoption, reference, and harmonization by existing regulatory frameworks, standards organizations, and governmental bodies. The following principles guide standards interoperability:

- **Adoption by Reference:** Regulatory frameworks may adopt CMOS-SB standards by reference, incorporating their requirements into existing compliance programs without duplication of content.
- **Harmonization:** Where existing standards address overlapping domains, CMOS-SB will publish harmonization guidance identifying areas of alignment, complementarity, and potential conflict.
- **Jurisdictional Adaptation:** CMOS-SB standards may be adapted by national or regional regulatory bodies to account for jurisdictional legal requirements, provided that adaptations do not reduce the baseline protections established by the original standards.
- **Cross-Reference:** Regulatory frameworks may cross-reference CMOS-SB standards in guidance documents, inspection protocols, or compliance checklists without formal adoption.

10.3 For Researchers and Academics

Emotional Epidemiology and the S-R-C Model provide research frameworks applicable across disciplines including cognitive science, public health, human-computer interaction, AI ethics, network science, organizational behavior, and social psychology. Researchers engaging with these frameworks are invited to build upon, test, extend, and critique the foundational work.

Primary Citation Guidance

Thompson, I.A. (2026). *Emotional Epidemiology: A Field Framework for Understanding Population-Level Emotional Dynamics*. Sugar Sands Publishing LLC / Sugar Sands Philanthropies Inc. DOI: 10.5281/zenodo.20314466. ORCID: 0009-0002-7213-3235.

Researchers are encouraged to engage with the CMOS-SB Standards Committee through the public comment process, to propose new empirical studies that would inform standards development, and to contribute to the working group processes that will develop the next generation of CMOS-SB standards. Academic engagement is a core pillar of the CMOS-SB public-interest mission: the standards are only as good as the science they are built on, and advancing the science advances the standards.

Appendices

Appendix A — Glossary of Terms

Term	Definition
Audit Visibility	The mode through which a control's performance is observable during audit: Direct, Aggregated, or Indirect.
Closed-Loop Control	A governance mechanism in which control performance is continuously monitored and findings are fed back to improve control design and organizational capability.
CMOS-SB	Cognitive Mode Operating System Standards Board. The world's first standards body governing the Human-Machine Layer — the interface at which digital systems interact with, influence, and shape human emotional states and cognitive modes.
CMSS	Cognitive Mode Stability Standard. CMOS-SB Standard 1002. Governs mode identification, transition safety, load balancing, drift detection, and recovery requirements.

Term	Definition
Cognitive Baseline	The stable operating range for a given deployment context, characterized by attentional bandwidth, emotional load tolerance, relational sensitivity, cognitive processing capacity, and environmental stress thresholds. Baselines are contextual, not personal.
Cognitive Mode	A discrete, identifiable state of human cognitive-emotional functioning characterized by distinct inputs, outputs, constraints, transition conditions, and failure conditions.
Cognitive Zero Trust	The emerging security maturity level (3.5+) at which the cognitive and emotional state of users becomes a first-class architectural consideration, extending traditional Zero Trust frameworks into the Human-Machine Layer.
Collective Resilience (C)	The third governing force in the S-R-C Model. The dampening force that reduces Susceptibility and Transmission Rate, built through relational trust, emotional safety design, and recovery mechanisms.
CMP-HC	Configuration Management Plan for Human Cognition. The operational doctrine that translates CMOS-SB standards into implementable, auditable controls. The world's first structured framework for governing cognitive and emotional interfaces between humans and intelligent systems.
Control Effectiveness Metric (CEM)	A percentage representing the proportion of validation events in which a control performed as required, calculated per control, per domain, and at aggregate program level.
EDCPS	Emotional Data Consent and Privacy Standard. CMOS-SB Standard 1004. Governs consent, minimization, retention, and anti-surveillance requirements for emotional data.
EISS	Emotional Infrastructure Safety Standard. CMOS-SB Standard 1001. Establishes baseline safety requirements for systems interacting with human emotional states.
Emotional Drift	Progressive, often gradual movement of a user or population away from established cognitive baselines, driven by cumulative system-level influences.
Emotional Epidemiology	An interdisciplinary scientific framework for understanding how emotional states emerge, propagate, and stabilize within human populations. Introduced by Isabelle Anne Thompson. DOI: 10.5281/zenodo.20314466.
Emotional Infrastructure	The technical and relational systems that mediate emotional and cognitive experience at scale — the substrate through which emotional experiences are shaped, transmitted, amplified, suppressed, and structured.
Emotional-Infrastructure System	Any digital system that interacts with, influences, or responds to human emotional states or cognitive modes at any scale.
Emotional-Risk Transmission	The propagation of emotional states, signals, or activations through a system or network in ways that may increase susceptibility, amplify distress, or accelerate drift.

Term	Definition
ETDS	Emotional Transparency and Disclosure Standard. CMOS-SB Standard 1003. Establishes mandatory disclosure requirements for systems that infer, respond to, or influence emotional states. Prohibits opaque emotional influence.
Governance Spine	The five foundational CMOS-SB standards pillars (EISS, CMSS, ETDS, EDCPS, PERMS) that together define the normative requirements for safe operation at the Human-Machine Layer.
Human-Machine Layer	The interface domain at which digital systems interact with, influence, and shape human emotional states and cognitive modes. The primary jurisdiction of CMOS-SB governance.
Joy Tracker	The first operational application of Emotional Epidemiology and the CMOS-SB reference implementation, demonstrating that emotional wellbeing tools can be built and CMOS-SB standards validated in practice.
Mode Collapse	A system-level failure condition in which a user or population loses access to the full range of cognitive modes and becomes locked in a contracted or overlocked state.
PERMS	Population-Level Emotional Risk Monitoring Standard. CMOS-SB Standard 1005. Establishes monitoring, detection, and reporting requirements for population-level emotional risk patterns.
Reference Architecture (RA-1.0)	The three-layer CMOS-SB architectural model: Governance Spine, Safeguard Layer, and Monitoring and Feedback Loop.
Safeguard	A technical or procedural control implemented to prevent, detect, or mitigate emotional or cognitive harm at the Human-Machine Layer.
S-R-C Model	The Susceptibility-Transmission Rate-Collective Resilience Model. The theoretical framework at the core of Emotional Epidemiology, describing the three governing forces of population-level emotional dynamics.
Susceptibility (S)	The first governing force in the S-R-C Model. The degree of vulnerability of a population or individual to emotional influence, drift, or contagion — a contextual, dynamic, systemic property.
Transmission Rate (R)	The second governing force in the S-R-C Model. The speed and intensity at which emotional states propagate through a population or network.

Appendix B — Standards Registry

Standard ID	Standard Name	Abbreviation	Version	Status	Effective Date
CMOS-SB 1001	Emotional Infrastructure Safety Standard	EISS	1.0	Active	June 9, 2026
CMOS-SB 1002	Cognitive Mode Stability Standard	CMSS	1.0	Active	June 9, 2026
CMOS-SB 1003	Emotional Transparency & Disclosure Standard	ETDS	1.0	Active	June 9, 2026
CMOS-SB 1004	Emotional Data Consent & Privacy Standard	EDCPS	1.0	Active	June 9, 2026
CMOS-SB 1005	Population-Level Emotional Risk Monitoring Standard	PERMS	1.0	Active	June 9, 2026

Appendix C — CMP-HC Domain Reference

Domain Name	Abbrev.	Control Prefix	Primary Objective	Regulatory Cross-Reference
Access & Identity Management	AIM	CMP-HC-AIM	Govern who may interact with emotional systems and under what conditions	HIPAA Administrative Safeguards; NIST AC; SOC 2 Security
Data Protection & Privacy	DPP	CMP-HC-DPP	Implement EDCPS requirements across emotional data lifecycle	HIPAA Technical Safeguards; HITECH; SOC 2 Privacy/Confidentiality
Change & Configuration Management	CCM	CMP-HC-CCM	Govern changes affecting cognitive mode behavior and safeguard function	21 CFR Part 11; NIST CM; SOC 2 Processing Integrity
Security Operations & Incident Management	SOIM	CMP-HC-SOIM	Detect, respond to, and recover from emotional safety incidents	HIPAA Breach Notification; NIST IR; Joint Commission
Business Continuity & Disaster Recovery	BCDR	CMP-HC-BCDR	Maintain emotional safety protections during system disruptions	HIPAA Contingency Plan; NIST CP; SOC 2 Availability
Regulatory Compliance & Audit Readiness	RCAR	CMP-HC-RCAR	Maintain continuous audit-readiness across applicable requirements	HITRUST CSF; NIST AU; SOC 2 Type II; CMS CoP

Appendix D — Translation Matrix Summary

CMP-HC Domain	CMOS-SB Governance Category	Primary Standard(s)	Relationship Type
AIM	User Protection Controls	EDCPS, EISS	Direct implementation
DPP	Information Governance	EDCPS	Direct implementation with traceability requirements
CCM	Operational Controls	CMSS, ETDS	Direct implementation with evidence rigor
SOIM	Oversight & Accountability	PERMS, EISS	Direct with escalation and reporting additions
BCDR	Operational Controls	EISS, CMSS	Direct with continuity-specific requirements
RCAR	Governance & Leadership	All	Aggregate — formalizes expectations across all domains

Appendix E — Traceability Schema Summary

Schema Domain	Abbrev.	Evidence Types	Retention Schedule	Cross-Domain Dependencies
Cognitive-Mode Safety	CMS	Mode logs, transition records, baseline deviation reports	3 years minimum	TI (telemetry), GC (governance)
Telemetry Integrity	TI	Monitoring data, anomaly detection logs, PERMS reports	3 years minimum	CMS (modes), OR (operations)
Governance Controls	GC	Policy records, approval documentation, audit trails	7 years minimum	All domains
Equity & Access	EA	Demographic coverage analysis, accessibility records, equity audit reports	3 years minimum	GC (governance), OR (operations)
Operational Readiness	OR	System readiness assessments, DR test results, CEM reports	3 years minimum	CMS, TI, GC

Schema Domain	Abbrev.	Evidence Types	Retention Schedule	Cross-Domain Dependencies
Adversarial Safety & Pen Testing	AS	Penetration test reports, adversarial simulation results, remediation records	5 years minimum	GC, OR, SOIM domain

Appendix F — Document Control

Field	Value
Document ID	CMOS-SB-FMD-001
Document Title	CMOS-SB Flagship Master Document
Version	1.0
Publication Date	June 9, 2026
Effective Date	June 9, 2026
Next Scheduled Review	June 9, 2027
Document Owner	CMOS-SB Governance Office
Standards Steward	Isabelle Anne Thompson
Author	Isabelle Anne Thompson
Hosted by	Sugar Sands Publishing LLC, Pensacola, FL
Philanthropic Affiliate	Sugar Sands Philanthropies Inc
ORCID	0009-0002-7213-3235
DOI Reference	10.5281/zenodo.20314466
Trademark Notice	Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC. All rights reserved.
Supersedes	No prior version
Classification	Public — Authoritative Master Document