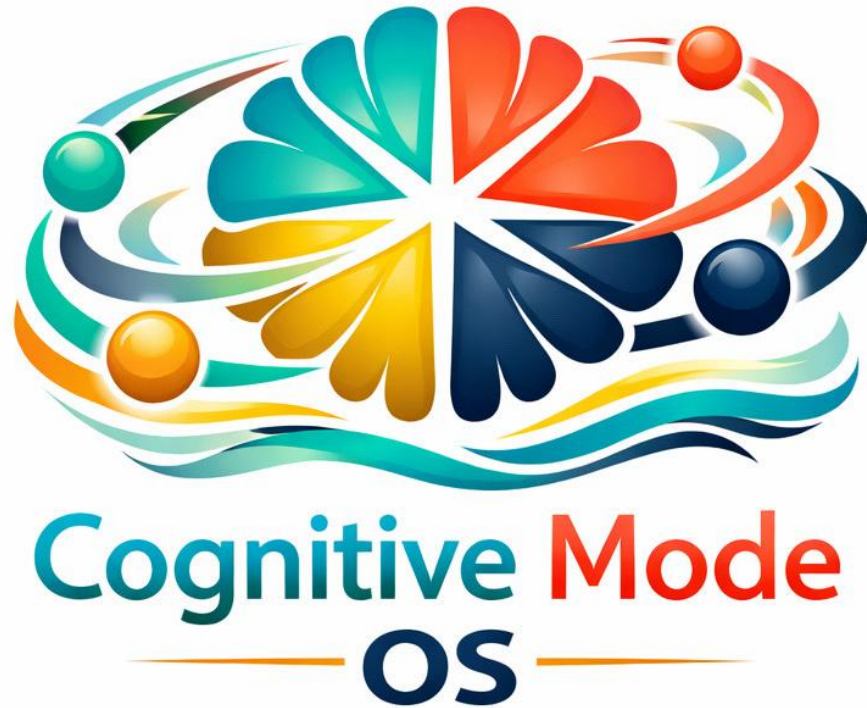




CMOS-SB Frequently Asked Questions

Publication Set Item 17 of 20 | Version 1.0 | July 26, 2026

Issued by: CMOS-SB Standards Committee

cmos-sb.org | Pensacola, FL

"The human-machine interface is the most consequential unregulated infrastructure on Earth. CMOS-SB exists to change that."

How to Use This Document

This FAQ provides answers to the most frequently asked questions about CMOS-SB, its scientific foundations, governance architecture, standards canon, and implementation pathway. It is organized into four audience sections: **General & Press**, **Enterprise & Organizational**, **Regulatory & Policy**, and **Technical & Developer**. Readers are encouraged to navigate directly to the section most relevant to their context.

Section 1: General & Press

For journalists, analysts, and members of the public seeking to understand what CMOS-SB is, why it was founded, and what it governs.

Q1. What is CMOS-SB?

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 function. Founded on July 26, 2026, CMOS-SB publishes auditable, science-grounded governance standards that organizations can implement, regulators can reference, and AI developers can build to. It is hosted by Sugar Sands Publishing LLC, Pensacola, FL, and founded and architected by Isabelle Anne Thompson.

Q2. What is the "Human-Machine Layer"?

The Human-Machine Layer is the interface domain where digital systems — including AI, adaptive platforms, and intelligent agents — directly interact with human attention, emotion, and cognitive function. Unlike physical or financial infrastructure, this layer has operated without governance standards. CMOS-SB defines what responsible behavior at that interface looks like, and how to measure, audit, and enforce it.

Q3. What problem is CMOS-SB solving?

Today's AI systems infer emotional states, adapt responses based on cognitive signals, modulate attention and mood, and shape relational dynamics for billions of users simultaneously — inside enterprises, healthcare systems, financial institutions, and consumer platforms. They do this with no standardized framework governing responsible behavior at that interface. The consequences are measurable, population-level, and accelerating. CMOS-SB closes this governance gap with a complete, auditable, science-grounded architecture.

Q4. Who founded CMOS-SB and when?

CMOS-SB was founded and architected by Isabelle Anne Thompson, Founder and Principal of Sugar Sands Publishing LLC and Founder of Sugar Sands Philanthropies Inc., based in Pensacola, FL. CMOS-SB officially launched on July 26, 2026, with the publication of its complete founding document, flagship master document, five governance spine standards, operational doctrine, compliance audit template, and supporting publication set.

Q5. What is Emotional Epidemiology?

Emotional Epidemiology is a scientific discipline that studies the patterns, transmission, and impact of emotions across individuals, communities, and populations. It establishes that emotional states propagate through populations in measurable, predictable, and governable ways — analogous to biological contagion dynamics. Susceptibility, Transmission Rate, and Collective Resilience (the S-R-C Model) govern whether AI-mediated environments trend toward stability or volatility at the population level. The foundational preprint is registered at DOI: 10.5281/zenodo.20314466.

Q6. What is the S-R-C Model?

The Susceptibility-Transmission-Collective Resilience (S-R-C) Model is the theoretical framework that describes how emotional dynamics operate through three core variables: **Susceptibility** — an individual's or group's openness to emotional influence at a given moment; **Transmission Rate** — the speed and fidelity with which an emotional signal moves from a system to a user or across a population; and **Collective Resilience** — the aggregate capacity of a population to absorb emotional inputs without systemic destabilization. Together, these variables determine whether a digital environment trends toward stability or contagion.

Q7. Is CMOS-SB affiliated with any government or regulatory body?

No. CMOS-SB is an independent standards body. It operates without affiliation to any government agency, political body, or commercial interest. Its governance architecture includes independence protections specifically designed to preserve scientific integrity and public-interest orientation. CMOS-SB standards may be referenced by regulators and policymakers, but CMOS-SB itself does not hold regulatory authority.

Section 2: Enterprise & Organizational

For Chief AI Officers, Chief Risk Officers, General Counsel, compliance teams, and enterprise leadership evaluating CMOS-SB for organizational readiness.

Q8. Why should my organization act on CMOS-SB now?

AI systems are already operating inside virtually every major organization — shaping how employees think, how customers feel, and how decisions get made. CMOS-SB provides the first structured governance framework for that layer. For organizations building FY27 strategic plans, the question is no longer whether AI governance at the human-machine layer will be required — it is whether your

organization will define the standard or be measured against someone else's. Early adopters gain first-mover advantage in compliance architecture, stakeholder trust, and regulatory positioning.

Q9. What does CMOS-SB compliance require?

CMOS-SB compliance is assessed across five Governance Spine Standards: **Emotional Infrastructure Safety (EISS)**, **Cognitive Mode Stability (CMSS)**, **Emotional Transparency & Disclosure (ETDS)**, **Emotional Data Consent & Privacy (EDCPS)**, and **Population-Level Emotional Risk Monitoring (PERMS)**. Each standard contains specific, auditable requirements. The Compliance Audit Template (Publication Set Item 13) provides a structured, evidence-based checklist mapped to all five standards, designed for use by internal compliance teams, independent auditors, and organizational leadership.

Q10. How does CMOS-SB relate to our existing AI governance and risk frameworks?

CMOS-SB is designed to complement, not replace, existing AI governance frameworks such as the NIST AI RMF, ISO/IEC 42001, and the EU AI Act. It addresses a specific gap those frameworks do not fully cover: the governance of emotional and cognitive impact at the human-machine interface. Organizations with mature AI governance programs will find CMOS-SB integrates cleanly as an additional compliance domain. Organizations earlier in their AI governance journey can use CMOS-SB as a structured entry point.

Q11. What is the CMP-HC and how does it support implementation?

The Configuration Management Plan for Human Cognition (CMP-HC) is CMOS-SB's operational doctrine — the implementation layer that translates governance standards into practical, auditable action. It is organized across six compliance domains: Emotional Infrastructure Safety, Cognitive Mode Stability, Transparency & Disclosure, Data Consent & Privacy, Population-Level Risk Monitoring, and Continuous Improvement. The CMP-HC provides baselines, safeguard specifications, monitoring requirements, traceability architecture, and audit procedures. It is the document compliance teams use to operationalize CMOS-SB standards day-to-day.

Q12. What is the Compliance Audit Template?

The CMOS-SB Compliance Audit Template (Item 13 of the Publication Set) is a structured, evidence-based checklist mapped to all five Governance Spine Standards. It is designed for internal compliance teams conducting self-assessments, independent auditors conducting formal audits, and organizational leadership preparing for regulatory review. Each checklist item includes a Standard Reference, a Yes/No/Partial/N/A response field, and a mandatory Notes/Evidence field requiring traceable documentation references. A Summary Scorecard is included to aggregate findings across all five standards.

Section 3: Regulatory & Policy

For policymakers, regulators, legislative staff, and policy researchers evaluating CMOS-SB as a reference framework or regulatory anchor.

Q13. What is CMOS-SB's regulatory standing?

CMOS-SB is a voluntary standards body — it publishes standards, not law. However, its governance architecture is specifically designed so that regulators can reference CMOS-SB standards in rulemaking, enforcement guidance, and procurement requirements. CMOS-SB operates as a science-grounded, auditable standard analogous to how NIST, ISO, or IEEE standards function in technical governance contexts — as the established baseline from which regulatory requirements are drawn.

Q14. How does CMOS-SB relate to the EU AI Act, NIST AI RMF, and other AI policy frameworks?

Existing frameworks address AI risk at the system level — accuracy, fairness, transparency, and safety of AI model outputs. CMOS-SB addresses a distinct and complementary domain: the governance of what happens at the interface between AI systems and human emotional and cognitive states. It does not duplicate existing frameworks; it fills the gap they do not cover. Regulators working on AI and mental health, AI and consumer protection, or AI and workplace safety will find CMOS-SB directly relevant.

Q15. Can CMOS-SB standards be cited in procurement requirements or vendor contracts?

Yes. CMOS-SB standards are published as fully specified, version-controlled governance documents with DOI registration and stable reference architecture. Organizations and government agencies can reference CMOS-SB standards (e.g., EISS-1001, CMSS-1002) in procurement requirements, vendor contracts, and third-party risk management programs exactly as they would reference ISO or NIST standards. The Compliance Audit Template provides the evidence framework for vendor self-attestation or independent audit.

Q16. What is the CMOS-SB standards development and versioning process?

CMOS-SB standards are developed through a ten-stage Standards Development Process (SDP) that includes: Identification, Scoping, Drafting, Internal Review, Scientific Review, Public Comment, Adjudication, Ratification, Publication, and Versioning. All ratified standards carry version numbers and planned review cycles. Version 1.0 of all five Governance Spine Standards was ratified and published on July 26, 2026, with a scheduled review date of July 26, 2027.

Section 4: Technical & Developer

For AI developers, platform engineers, product teams, and technical architects designing or auditing human-machine interface systems.

Q17. What are the five CMOS-SB Governance Spine Standards?

- **EISS (CMOS-SB-1001) — Emotional Infrastructure Safety Standard:** Governs baseline safeguards to prevent harmful emotional impact from system outputs. Includes impact throttling requirements, misinterpretation mitigation, and amplification controls.
- **CMSS (CMOS-SB-1002) — Cognitive Mode Stability Standard:** Governs requirements to preserve cognitive stability and prevent overload, drift, and destabilization. Anchored to the Cognitive Mode Quadrant framework (Open, Neutral, Contracted, Overclocked states).

- **ETDS (CMOS-SB-1003) — Emotional Transparency & Disclosure Standard:** Requires systems to disclose when emotional or cognitive inference is occurring, and to maintain transparency about adaptive behaviors affecting user emotional state.
- **EDCPS (CMOS-SB-1004) — Emotional Data Consent & Privacy Standard:** Governs the collection, storage, use, and minimization of emotional and cognitive data, including consent frameworks and data lifecycle controls.
- **PERMS (CMOS-SB-1005) — Population-Level Emotional Risk Monitoring Standard:** Requires systems operating at scale to monitor for population-level emotional risk signals, including contagion acceleration, anomaly clustering, and volatility spikes.

Q18. What are the CMOS-SB Safeguard Design Patterns?

CMOS-SB defines six modular safeguard design patterns that serve as implementation building blocks for compliant systems:

- **(1) Emotional-Impact Throttling** — prevents sudden spikes in emotional intensity at the output layer.
- **(2) Cognitive-Load Balancing** — prevents cognitive overload from multi-modal or high-velocity input.
- **(3) Contextual Sensitivity Filter** — reduces misinterpretation and emotional drift at the processing layer.
- **(4) Relational Integrity Guardrail** — ensures tone, empathy boundaries, and relational safety.
- **(5) Drift Detection & Correction Loop** — detects and corrects emotional or cognitive drift in real time.
- **(6) Population-Level Anomaly Detection** — identifies contagion spikes, clustering, and population-level risk signals.

These patterns are defined in the Safeguard Design Pattern Set (CMOSSB v1.0).

Q19. What is Joy Tracker and why does it matter?

Joy Tracker is CMOS-SB's reference implementation — a real-world consumer product that demonstrates CMOS-SB standards in live operation, validates governance patterns in practice, and generates real-world evidence for the ecosystem. It is the fifth and final line of the CMOS-SB five-line ecosystem, serving as the proof-of-concept that the science, theory, and standards can operate in the real world. For developers, Joy Tracker functions as a working reference architecture for emotionally responsible product design.

Q20. How does CMOS-SB address the Zero Trust security model?

CMOS-SB introduces the concept of **Cognitive Zero Trust** as the next evolution of security maturity — extending the Zero Trust principle ("never trust, always verify") from network and identity layers to the cognitive and emotional layer. At maturity level 3.5+, Cognitive Zero Trust incorporates Cognitive Permissions, Human + AI Signals, and Emotional Security as core trust context variables. CMOS-SB standards provide the governance architecture for organizations seeking to implement Cognitive Zero Trust in their AI-integrated environments.

Additional Resources

The following documents are available at **cmos-sb.org** as part of the CMOS-SB Publication Set (Version 1.0, June 9, 2026):

- CMOS-SB Flagship Master Document (FMD-001)
- CMOS-SB Founding Document (FD-001)
- Governance Spine Standards: EISS-1001, CMSS-1002, ETDS-1003, EDCPS-1004, PERMS-1005
- CMP-HC Operational Doctrine
- Compliance Audit Template
- Public Comment Submission Form

- Standards Roadmap (Year 1–3)
- Executive Briefing Deck
- Media Kit: One-Pager Fact Sheet & Boilerplate

Contact & Public Comment

CMOS-SB welcomes stakeholder engagement. To submit public comment, request briefings, or inquire about organizational engagement, visit **cmos-sb.org**.

CMOS-SB is hosted by **Sugar Sands Publishing LLC**, Pensacola, FL.

© 2026 Sugar Sands Publishing LLC. All rights reserved. Cognitive Mode OS™ is a trademark of Isabelle Anne Thompson / Sugar Sands Publishing LLC.