



CMOS-SB

Governing the Human-Machine Layer

EXECUTIVE BRIEFING • JULY 2026

AI Is Already Inside Your Organization.

🔗 Is It Governed?



PHYSICAL INFRASTRUCTURE

Safety codes govern every beam, wire, and pipe.

Building standards. Fire codes. Structural audits.
Mandatory compliance.

✓ GOVERNED



FINANCIAL SYSTEMS

Capital requirements and stress-testing
govern every dollar.

Basel III. Dodd-Frank. SEC oversight. Systemic risk
monitoring.

✓ GOVERNED



HUMAN-MACHINE INTERFACE

**No governance framework existed
—
until today.**

Billions of users. Zero standards. Until CMOS-SB.

⚠ UNGOVERNED — UNTIL NOW

■ AI systems are shaping how employees think, how customers feel, and how decisions are made — at unprecedented scale and speed.

Emotional States Propagate Like Contagion.

A Measurable, Governable Phenomenon.

EMOTIONAL EPIDEMIOLOGY

A scientific discipline studying the **patterns, transmission, and impact** of emotions across individuals, communities, and populations. Emotional states propagate in **measurable, predictable, and governable** ways — analogous to biological contagion dynamics.

S-R-C MODEL — CORE VARIABLES

S

Susceptibility

Individual & system vulnerability to emotional influence.

R

Transmission Rate

Speed & spread of emotional states through populations.

C

Collective Resilience

System capacity to trend toward stability vs. volatility.



AI-mediated environments act as **high-speed transmission vectors** — accelerating emotional spread at unprecedented scale. Governing these systems requires the same precision as governing biological contagion.

DOI 10.5281/zenodo.20314466

THE CMOS-SB ECOSYSTEM IN FIVE LINES

SCIENCE. THEORY. STANDARDS. IMPLEMENTATION. REAL-WORLD IMPACT.



1. EMOTIONAL EPIDEMIOLOGY

EXPLAINS WHAT IS HAPPENING.

A scientific discipline that studies the **patterns, transmission, and impact** of emotions across individuals, communities, and populations.



2. SRC MODEL

EXPLAINS HOW IT HAPPENS.

A theoretical model that describes the **Susceptibility, Transmission, and Resilience** dynamics that shape emotional and cognitive experiences.



3. CMOS-SB

DEFINES WHAT RESPONSIBLE SYSTEMS **SHOULD DO** ABOUT IT.

A standards body that establishes **governance, safeguards, and requirements** to protect emotional and cognitive wellbeing at the Human-Machine Layer.



4. CMP-HC

DEFINES HOW TO **IMPLEMENT AND AUDIT** THOSE RESPONSIBILITIES.

An operational doctrine that turns standards into practical actions through **baselines, safeguards, monitoring, and continuous improvement**.



5. JOY TRACKER

PROVES THE IDEAS CAN OPERATE IN THE **REAL WORLD**.

A **reference implementation** that demonstrates emotional wellbeing tools, validates standards in practice, and generates **real-world evidence**.



TOGETHER, THESE FIVE ELEMENTS CREATE A COMPLETE ECOSYSTEM THAT ADVANCES EMOTIONAL SAFETY, COGNITIVE STABILITY, AND COLLECTIVE RESILIENCE.

CMOS-SB

HUMAN-MACHINE LAYER GOVERNANCE



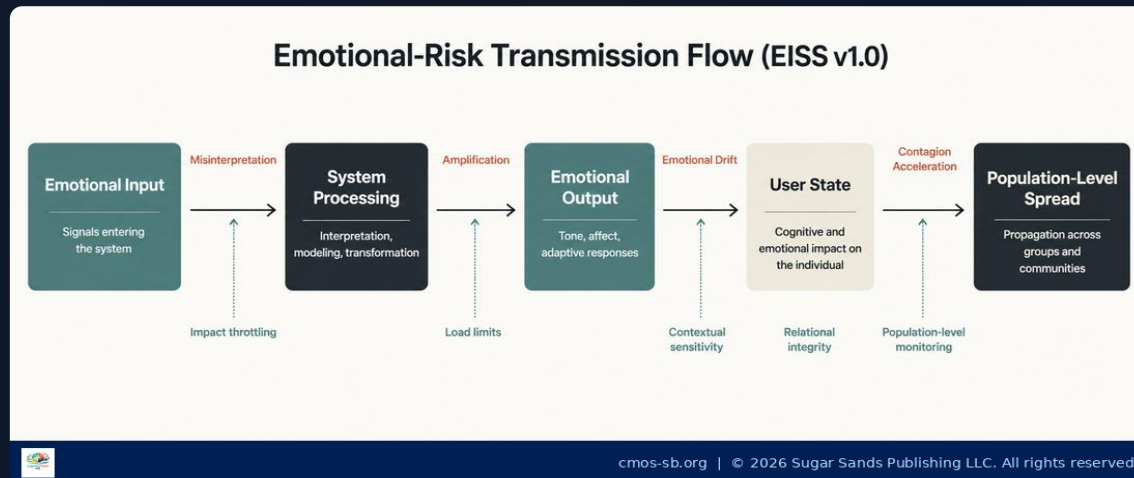
cmos-sb.org | © 2026 Sugar Sands Publishing LLC. All rights reserved.



The CMOS-SB Ecosystem in Five Lines:

Science → Theory → Standards → Implementation → Real-World Impact

From Input to Population: **The Transmission Flow**

**RISK STAGE 1**

Misinterpretation at the input layer amplifies risk.

**RISK STAGE 2**

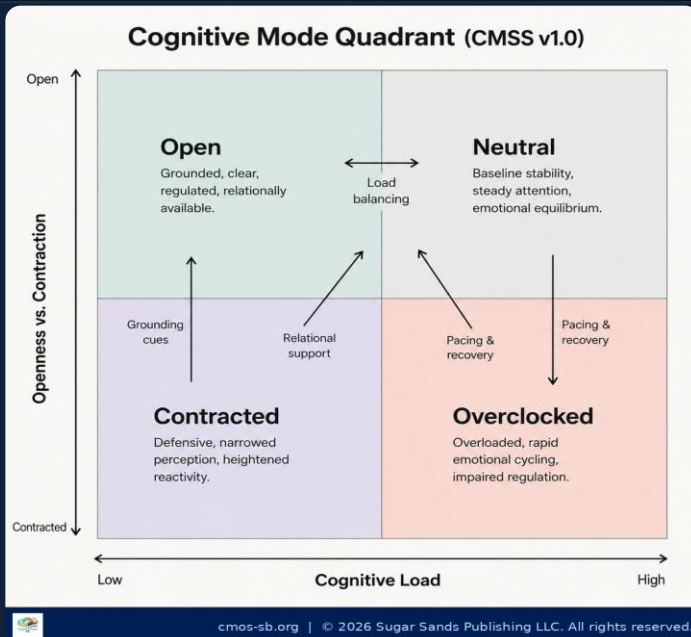
Amplification at the processing layer accelerates spread.

**RISK STAGE 3**

Contagion at population level is measurable and governable.

Understanding Cognitive States at the Interface

Four measurable cognitive states that responsible AI systems must detect, respond to, and protect.



CMSS V1.0



Target States: Open + Neutral

Grounded, stable, and relationally available — optimal conditions for human-machine engagement.



Risk States: Contracted + Overclocked

Defensive, overloaded, and cognitively impaired — require AI-side safeguards and intervention.



Responsible AI design must detect, respond to, and protect all four cognitive states.

Security Has Evolved. Cognitive Governance Is Next.



 CMOS-SB defines the governance architecture for Maturity Level 3.5+: Cognitive Zero Trust.

3.5+ ADDS



Cognitive Permissions

3.5+ ADDS



Human + AI Signals

3.5+ ADDS



Emotional Security

 Organizations at every maturity level can begin CMOS-SB compliance today.



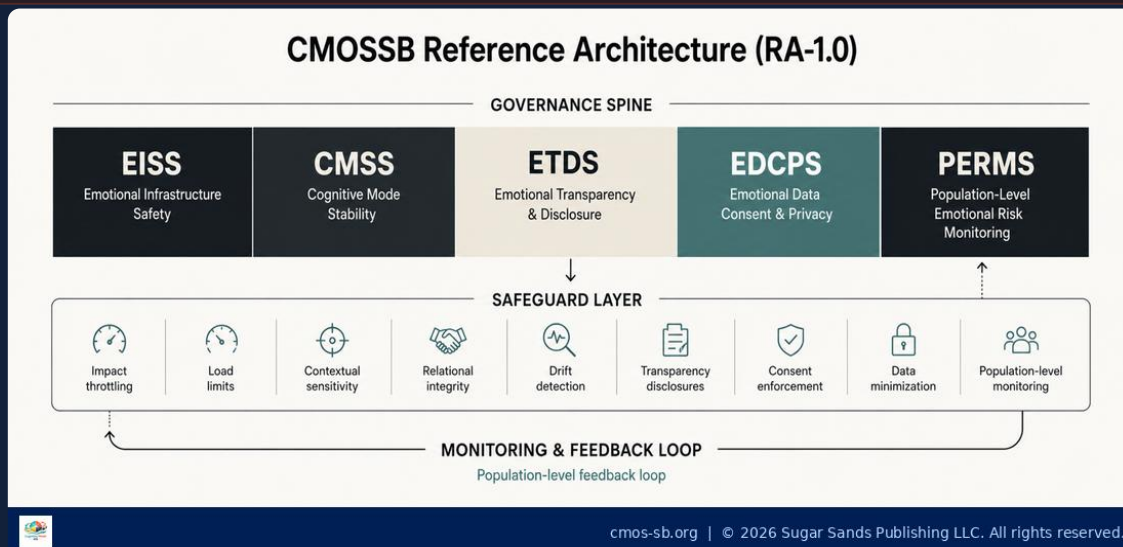
Five Auditable Standards. One Governance Architecture.

The Governance Spine — Full Specification, Version 1.0

EISS-1001 v1.0 · Jul 2026	1 Emotional Infrastructure Safety Standard Pillar 1 — Baseline emotional impact safeguards for all human-machine interfaces.	PUBLISHED	
CMSS-1002 v1.0 · Jul 2026	2 Cognitive Mode Stability Standard Pillar 2 — Cognitive mode detection and protection across all four quadrant states.	PUBLISHED	
ETDS-1003 v1.0 · Jul 2026	3 Emotional Transparency & Disclosure Standard Pillar 3 — Mandatory transparency requirements about emotional inference and state modeling.	PUBLISHED	
EDCPS-1004 v1.0 · Jul 2026	4 Emotional Data Consent & Privacy Standard Pillar 4 — Emotional data governance, consent frameworks, and privacy protections.	PUBLISHED	
PERMS-1005 v1.0 · Jul 2026	5 Population-Level Emotional Risk Monitoring Standard Pillar 5 — Population-scale emotional risk detection, measurement, and response protocols.	PUBLISHED	

From Standards to System: The CMOS-SB Reference Architecture

RA-1.0 — Governance Spine + Safeguard Layer + Monitoring Loop



GOVERNANCE SPINE

5 Standards Pillars

Defining what responsible human-machine systems must do — EISS, CMSS, ETDS, EDCPS, PERMS.

FOUNDATIONAL

SAFEGUARD LAYER

Operational Controls

Translating standards into system behaviors — throttling, load balancing, consent enforcement, drift detection.

IMPLEMENTATION

MONITORING & FEEDBACK LOOP

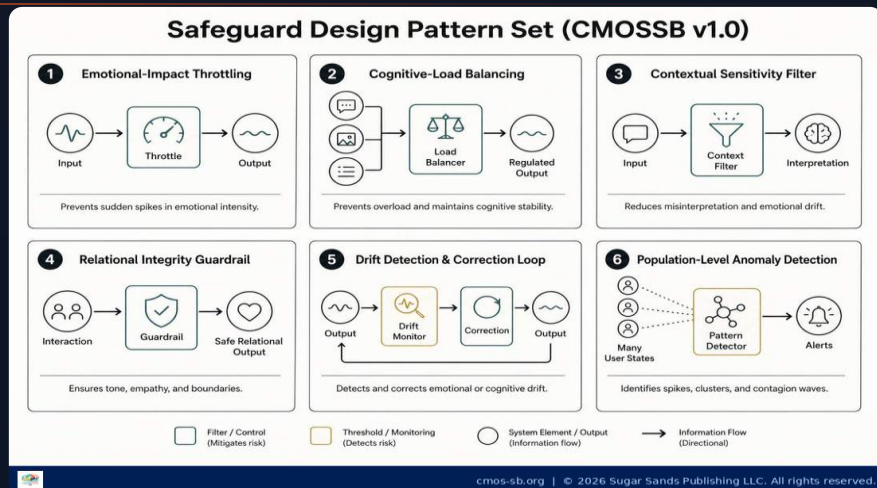
Population-Level Oversight

Continuous real-world feedback detecting population-scale emotional risk signals and triggering corrective response.

CONTINUOUS

Six Modular Safeguards. Implementation-Ready.

CMOSSB Safeguard Design Pattern Set v1.0



SAFEGUARDS 1-3

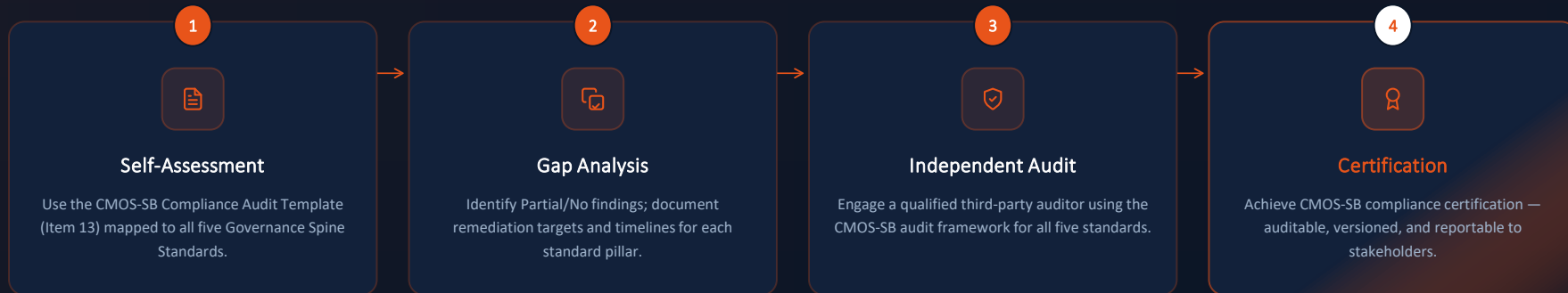
- Emotional-Impact Throttling — prevents sudden spikes in emotional intensity
- Cognitive-Load Balancing — prevents overload, maintains cognitive stability
- Contextual Sensitivity Filter — reduces misinterpretation and emotional drift

SAFEGUARDS 4-6

- Relational Integrity Guardrail — ensures tone, empathy, and relational boundaries
- Drift Detection & Correction Loop — detects and corrects emotional or cognitive drift
- Population-Level Anomaly Detection — identifies spikes, clusters, and contagion waves

⚡ Each pattern is modular, mappable to a Governance Spine standard, and deployable independently.

From Assessment to Certification: A Clear Compliance Path



WHO THIS APPLIES TO

ENTERPRISE

AI systems affecting employees, customers, or public-facing users at any scale or deployment.

REGULATED INDUSTRIES

Healthcare · Finance · Public Sector · Education — where emotional-AI risk carries regulatory exposure.

<> DEVELOPERS

Any platform deploying AI that models, infers, or responds to human emotional or cognitive signals.

CMOS-SB Is Relevant Across Every Sector

THREE PRIMARY AUDIENCES · ONE GOVERNANCE FRAMEWORK

AUDIENCE 01

Enterprise

Your AI tools are already inside your organization — shaping how employees think, how customers feel, and how decisions are made. CMOS-SB gives you the governance framework to manage them responsibly.

Get ahead of the regulatory curve. Protect your employees and customers before compliance becomes mandatory.

Begin with the Compliance Audit Template ->

AUDIENCE 02

Regulators & Policy

CMOS-SB provides the first auditable, science-grounded standard for human-machine layer oversight — built on peer-reviewed emotional epidemiology and a published governance spine.

Reference directly in rulemaking, procurement requirements, and enforcement guidance. No gaps to fill — the framework is complete.

Cite CMOS-SB standards directly in policy ->

AUDIENCE 03

Developers

Build to a standard. CMOS-SB defines exactly what responsible emotional-impact design looks like — and gives you a clear, provable path to demonstrate it.

Use the Safeguard Design Patterns and Reference Architecture RA-1.0 to implement governance at the system level, not as an afterthought.

Implement RA-1.0 and the six design patterns ->

A Complete Ecosystem: Science to Real-World Impact

THE CMOS-SB ECOSYSTEM IN FIVE LINES

SCIENCE. THEORY. STANDARDS. IMPLEMENTATION. REAL-WORLD IMPACT.



1. EMOTIONAL EPIDEMIOLOGY
EXPLAINS WHAT IS HAPPENING.

A scientific discipline that studies the **patterns**, **transmission**, and **impact** of emotions across individuals, communities, and populations.



2. SRC MODEL
EXPLAINS HOW IT HAPPENS.

A theoretical model that describes the **Susceptibility**, **Transmission**, and **Resilience** dynamics that shape emotional and cognitive experiences.



3. CMOS-SB
DEFINES WHAT RESPONSIBLE
SYSTEMS **SHOULD DO** ABOUT IT.

A standards body that establishes **governance**, **safeguards**, and **requirements** to protect emotional and cognitive wellbeing at the Human-Machine Layer.



4. CMP-HC
DEFINES HOW TO **IMPLEMENT** AND
AUDIT THOSE RESPONSIBILITIES.

An operational doctrine that turns standards into practical actions through **baselines**, **safeguards**, **monitoring**, and **continuous improvement**.



5. JOY TRACKER
PROVES THE IDEAS CAN OPERATE
IN THE **REAL WORLD**.

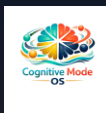
A **reference implementation** that demonstrates emotional wellbeing tools, validates standards in practice, and generates **real-world evidence**.



*TOGETHER, THESE FIVE ELEMENTS CREATE A COMPLETE ECOSYSTEM
THAT ADVANCES EMOTIONAL SAFETY, COGNITIVE STABILITY, AND COLLECTIVE RESILIENCE.*

CMOS-SB

HUMAN-MACHINE LAYER GOVERNANCE



The Human-Machine Interface Is the Most Consequential Unregulated Infrastructure on Earth.

CMOS-SB exists to change that.

NEXT STEPS



VISIT

cmos-sb.org

Full publication set available at launch — all 20 items including standards, reference architecture, design patterns, compliance audit template, and implementation guidance.



ENGAGE

Submit public comment

Request a briefing

Begin compliance assessment using the CMOS-SB Audit Template — mapped to all five standards, fully published and ready to use.



BUILD TO

Reference the standards Implement the architecture

Certify your systems. Use RA-1.0, the six Safeguard Design Patterns, and the five-pillar Governance Spine to build and demonstrate responsible compliance.