

COMPLIANCE MAPPING GUIDE

Regulatory Framework Alignment for AI Governance

Shadow Defend provides browser-based AI governance, helping enterprise security and compliance teams discover Shadow AI, maintain defensible audit trails, and demonstrate regulatory alignment.

Published 2026 | Enterprise AI Governance | shadowdefend.com/compliance

EXECUTIVE SUMMARY

AI Adoption Is Outpacing Oversight

THE CHALLENGE

Enterprise teams are adopting AI tools faster than governance programs can adapt. Employees access generative AI, code assistants, and data analysis platforms through their browsers every day, often before security, compliance, or procurement teams have evaluated the risk.

THE OPPORTUNITY

Shadow Defend closes this visibility gap. Through browser-based monitoring, it provides continuous discovery of AI tool usage, sensitive data detection, vendor risk visibility, and the comprehensive audit trails that compliance teams need for assessments, audits, and regulatory inquiries.

This guide shows how Shadow Defend aligns to twelve major regulatory and assurance frameworks, making it easier for buyers, compliance leaders, and security stakeholders to understand where the platform delivers direct coverage, supporting evidence, and operational value.

CORE CAPABILITIES

• AI application discovery and inventory	• Shadow AI detection and alerting
• Sensitive data monitoring	• AI vendor risk visibility and scoring
• Real-time usage monitoring	• Comprehensive audit trails
• Policy-based warnings and controls	• Compliance reporting and evidence collection

FRAMEWORK COVERAGE

Alignment at a Glance

The table below summarizes how Shadow Defend maps to each covered regulatory framework. Detailed per-control mappings follow in subsequent sections.

FRAMEWORK	PRIMARY BENEFIT	ALIGNMENT LEVEL
ISO 42001	AI governance, risk assessment, continuous monitoring, and impact documentation	Partial
ISO 27001	Security monitoring, audit logging, cloud service governance, and change management	Partial
ISO 27701	Privacy impact assessments, processing records, and personal data visibility	Partial
ISO 27017	Cloud service visibility and monitoring of AI service providers	Partial
ISO/IEC 27090	AI threat detection, input screening, and logging and monitoring evidence for organizations using AI	Full / Partial / Supporting
SOC 2	AI data flows, vendor oversight, confidentiality risk detection, and operational monitoring	Partial
HIPAA	PHI monitoring, audit evidence, and AI inventory for healthcare environments	Partial
PCI DSS	AI service inventory, access reviews, and cardholder data environment awareness	Partial / Supporting
CIS Controls	AI software inventory and detection of unauthorized applications	Full / Partial
FISMA / NIST	Continuous monitoring and automated AI risk oversight for federal systems	Partial
NIST AI RMF 1.0	AI system inventory, actual-usage monitoring, privacy-risk detection, and post-deployment oversight evidence	Full / Partial / Supporting
IEEE 2863	Usage-side AI governance evidence for the governing body of organizations that use AI	Supporting / Partial

ALIGNMENT KEY

Shadow Defend monitors AI tool usage through browser-based detection. In this guide, coverage marked as "Full" applies specifically to browser extensions and web applications, "Partial" indicates browser-based monitoring that supports the requirement, but organizations may need additional controls for non-browser access, and "Supporting" indicates indirect benefit that aids compliance without serving as the primary control.

Full	Shadow Defend directly addresses this requirement. For software inventory this applies to browser extensions and web applications.
-------------	--

Partial	Shadow Defend supports this requirement within browser-based contexts; additional controls may be needed for complete coverage.
Supporting	Shadow Defend provides indirect benefit that aids compliance efforts but is not the primary control.

ISO 27001**Information Security Management***International standard for managing information security risk across the enterprise*

Shadow Defend helps organizations meet ISO 27001 requirements by maintaining an inventory of AI tools accessed via browser, monitoring their usage, and generating audit trails for information security controls. It surfaces shadow AI with potential vulnerabilities, detects new AI services entering the environment, and supports evidence collection for formal ISMS assessments.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
A.5.23	Information security for cloud services	Detects unsanctioned AI tools and tracks sanctioned AI usage accessed via web browsers	Partial
A.8.8	Management of technical vulnerabilities	Identifies Shadow AI tools with potential security vulnerabilities and data exfiltration risks	Partial
A.8.15	Logging	Maintains audit trails of browser-based AI interactions for security event analysis	Partial
A.8.16	Monitoring activities	Real-time monitoring of AI tool usage in browsers with anomaly detection	Partial
A.8.32	Change management	Automatically detects new AI tools entering the organization via browser access, supporting change control processes	Partial

ISO 27701**Privacy Information Management***Extension of ISO 27001 establishing requirements for PII controllers and processors*

Shadow Defend supports privacy compliance by identifying what personal data is being processed by AI tools in browsers and maintaining audit logs that serve as evidence of AI-related data processing activities, including the ability to feed detection data into privacy impact assessments.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
7.2.1	Identify lawful basis for processing	Shows what personal data is being processed by AI tools, supporting lawful basis documentation	Supporting
7.3.2	Processing records	Audit logs serve as evidence of browser-based AI data processing activities	Partial
7.5.1	Privacy impact assessments	Detection data feeds privacy impact assessments for AI tool usage	Partial

ISO 42001

AI Management System

International standard for establishing and improving AI governance within organizations

Shadow Defend directly addresses ISO 42001 requirements for AI system monitoring, risk assessment, and impact documentation within browser-based contexts, the core layer of AI governance for web-accessed tools. It provides the continuous visibility and risk scoring that AI governance programs require.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
6.1.2	AI risk assessment	Risk scoring and classification of AI tools accessed via browser aligns with AI-specific risk evaluation requirements	Partial
8.2.1	AI impact assessment	Monitoring data provides evidence for AI system impact documentation	Partial
9.1.2	Monitoring AI systems	Core purpose. Monitors AI system usage in browsers with anomaly detection	Partial
A.6.3	AI system deployment	Detects and tracks AI tools deployed or accessed via browser	Partial

ISO 27017

Cloud Security

Cloud-specific security controls extending ISO 27002

Shadow Defend monitors AI cloud service usage in browsers and maintains visibility into which cloud AI services process company and customer data, helping organizations understand shared responsibility boundaries between themselves and their AI service providers.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
CLD.6.3.1	Shared roles & responsibilities	Documents which AI services process company and customer data, clarifying responsibility boundaries	Supporting
CLD.12.4.5	Monitoring of cloud services	Monitors AI cloud service usage and data flows in browsers for security visibility	Partial

ISO/IEC 27090**AI Security Threats**

Guidance on addressing security threats and compromises to AI systems (ISO/IEC 27090:2026)

ISO/IEC 27090 addresses attacks against AI systems, so most of its mitigations belong to the organizations that build those systems. Shadow Defend contributes where organizations use third-party AI via the browser: it maintains the inventory of AI systems and their use that Clause 5.2 calls for, screens model inputs for sensitive data before they leave the organization, and supplies the logging, monitoring, and alerting mitigations Clause 7 recommends.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
5.2	Inventory of AI systems and their use	Auto-discovers and maintains the inventory of AI systems and their use that Clause 5.2 calls for, covering browser-accessed tools	Full
5.2	AI governance programme	Tool risk scoring, usage monitoring, and audit evidence feed the risk analysis and monitoring parts of the AI governance program; the rest of the program remains with the organization	Supporting
5.5	Supply chain management	Inventories and monitors third-party AI services accessed via browser, supporting AI supply-chain threat visibility	Supporting
Clause 6	Types of potential compromise to AI systems	Most compromises in this clause are mitigated within the AI system itself; at the usage boundary, prompt inspection detects confidential data disclosed through model inputs	Supporting
Clause 7	Mitigations: logging, monitoring, input detection	Real-time monitoring, anomaly alerting, and exportable interaction logs provide the logging and monitoring mitigations; prompt inspection adds input screening at the usage layer	Partial

HIPAA**Health Insurance Portability and Accountability Act**

National standards for protecting sensitive patient health information

Shadow Defend helps healthcare organizations maintain HIPAA compliance by detecting PHI transmitted to unsanctioned AI tools via browser and maintaining audit trails for compliance evidence. The 2025 HHS proposed rule introduces an explicit AI inventory requirement, Shadow Defend directly supports this emerging obligation.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
§ 164.312(b)	Audit controls	Maintains logs of browser-based AI interactions involving PHI	Partial

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
§ 164.312(d)	Access controls	Identifies sanctioned vs. unsanctioned AI tool usage to inform access policy enforcement	Supporting
§ 164.312(e)(1)	Transmission security	Detects PHI transmitted to unsanctioned AI services via browser	Partial
HHS Proposed (2025)	AI inventory requirement	Maintains inventory of AI tools accessed via browser that may touch PHI	Partial

SOC 2

Service Organization Control 2

Trust Service Criteria: Security, Availability, Confidentiality, Processing Integrity, and Privacy

Shadow Defend addresses SOC 2 criteria by providing visibility into browser-based AI tool usage, maintaining audit trails, and detecting potential data disclosure to third-party AI services, supporting both vendor oversight and data transmission security across Trust Service Criteria.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
CC6.1	Logical access controls	Tracks browser-based AI tool access and associated data flows	Partial
CC7.1	System operations monitoring	Real-time monitoring of AI data transmissions in browsers	Partial
CC9.2	Vendor monitoring	Maintains inventory of AI vendors with risk assessments	Partial
CC6.7	Data transmission	Monitors data sent to AI providers in browsers; identifies sensitive data exfiltration	Partial
CC6.8	Unauthorized disclosure	Detects confidential data sharing with unsanctioned AI tools in browsers	Partial

PCI DSS**Payment Card Industry Data Security Standard***Security requirements for organizations handling cardholder data*

Shadow Defend helps organizations maintain PCI DSS compliance by monitoring AI tool usage in browsers within cardholder data environments and maintaining service provider inventories, providing the visibility needed to assess risk and support access control reviews.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
7.2	Least privilege access	Identifies AI tools with excessive data access, supporting access control reviews	Supporting
8.2–8.6	User authentication	Logs AI service account usage in browsers; detects unauthorized accounts	Supporting
12.8.1	Service provider inventory	Maintains inventory of AI service providers accessed via browser	Partial

CIS CONTROLS**Center for Internet Security Controls***Prioritized cybersecurity best practices for defending against common threats*

Shadow Defend addresses CIS Controls for asset and software inventory, the foundation of any security program by discovering and cataloging AI tools accessed via browser, including unauthorized applications that may bypass existing controls.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
1.1	Establish asset inventory	Discovers and catalogs AI tools accessed via browser across the organization	Partial
2.1	Establish software inventory	Maintains inventory of AI applications and browser extensions	Full
2.3	Unauthorized software	Detects and alerts on unsanctioned AI tools accessed via browser	Partial

FISMA / NIST**Federal Information Security Modernization Act***NIST Risk Management Framework and NIST SP 800-53 security controls for federal systems*

Shadow Defend addresses FISMA continuous monitoring requirements and supports NIST SP 800-53 AI system overlays for automated monitoring and risk assessment of browser-accessed AI tools, helping federal agencies and contractors demonstrate ongoing compliance posture.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
SI-04(02)	System monitoring, automated analysis	Real-time monitoring of browser-based AI tool usage with anomaly detection	Partial
CA-07	Continuous monitoring	Ongoing monitoring of AI-related risks and controls for browser-accessed tools	Partial

NIST AI RMF 1.0

Artificial Intelligence Risk Management Framework 1.0

Voluntary US framework for managing AI risks (NIST AI 100-1, January 2023), organized into four functions: GOVERN, MAP, MEASURE, and MANAGE. Widely referenced in enterprise AI policies, federal guidance, and insurer underwriting questions.

Shadow Defend supports AI RMF outcomes at the usage layer, where employees interact with external AI systems: it builds the AI system inventory GOVERN 1.6 calls for, provides continuous actual-usage monitoring and emergent-risk tracking (MEASURE 3.1), privacy-risk visibility (MEASURE 2.10), and the policy actions, alerts, and audit evidence MANAGE expects. It does not perform testing, evaluation, verification, and validation (TEVV) of AI models themselves; that remains the responsibility of the organizations that own those systems.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
GOVERN 1.6	Inventory AI systems	Automatically discovers and maintains an inventory of AI tools accessed via browser, including tools absent from approved lists	Full
GOVERN 4.2	Document risks and potential impacts of AI technology in use	Monitoring data and audit trails document which browser tools employees use and what data reached them	Supporting
GOVERN 4.3	Incident identification and information sharing	Real-time alerts and shareable audit evidence support incident identification and information sharing	Supporting
GOVERN 6.1	Third-party AI risk policies	Inventory and monitoring data support policies addressing AI risks from third-party entities	Supporting
GOVERN 6.2	Contingency for high-risk third-party incidents	Instant alerting and browser-layer controls support responses to incidents or failures in high-risk third-party AI systems	Supporting
MAP 4.1	Map risks for all AI system components, including third-party software	Discovers browser-accessed third-party AI tools, feeding the risk mapping of third-party components	Supporting
MAP 4.2	Identify and document internal risk controls	Warn/block policy actions and audit trails document usage-layer risk controls for third-party AI tools	Supporting
MEASURE 3.1	Track existing and emergent AI risks over time	Real-time monitoring and alerting track actual AI tool usage in deployed contexts, including personal accounts and newly adopted tools	Partial

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
MEASURE 2.10	Privacy risk of AI systems examined and documented	Inspects prompts for PII, credentials, and secrets before they reach AI providers; audit logs document resulting exposure	Partial
MANAGE 4.1	Post-deployment monitoring, incident response, and override	Policy-based warn/block actions, instant alerts to Slack, email, webhooks, or SIEM, and exportable audit evidence support post-deployment monitoring	Partial
MANAGE 3.1	Third-party AI risks and benefits regularly monitored	Continuously monitors third-party AI tool usage reached via browser and applies and documents browser-layer risk controls	Partial

IEEE 2863

Organizational Governance of AI

Recommended practice for organizational governance of artificial intelligence (IEEE 2863-2026)

IEEE 2863 frames AI governance as an activity of the governing body, covering organizations that use AI as much as those that build it. Shadow Defend gives the governing body its operating picture: what AI tools are in use, how they are being used, enforcement of usage policy through warn and block actions, and audit evidence that governance decisions were carried out.

CONTROL	REQUIREMENT	SHADOW DEFEND COVERAGE	ALIGNMENT
Principles	Security, accountability, and human oversight of AI use	Usage monitoring and per-interaction audit evidence give the governing body oversight of the AI tools employees actually use	Supporting
Processes	Life-cycle oversight, auditing, and incident response	Continuous monitoring, real-time alerts, and exportable audit trails support AI-use oversight and post-incident evidence	Partial
Processes	Value chain management	Inventories and monitors third-party AI services accessed via browser, including accounts and data flows	Supporting

SCOPE CONSIDERATIONS

What Shadow Defend Covers

Shadow Defend focuses on the browser, where much of today’s unsanctioned AI adoption begins. This approach addresses the most common vector for Shadow AI in enterprise environments, where employees are accessing generative AI tools, coding assistants, browser extensions, and AI-enabled SaaS experiences

Coverage marked as "Full" in this guide applies specifically to browser extensions and web applications. Organizations requiring governance of native desktop applications, infrastructure-level AI services, or identity management tooling may need additional controls to achieve complete coverage for specific framework requirements.

For many organizations, this makes Shadow Defend the fastest path to visibility and governance. Where broader coverage is required, such as native desktop applications, infrastructure-level AI services, or identity-layer enforcement, teams may pair Shadow Defend with additional controls to achieve end-to-end coverage.

A note on standards timing: EN 18286:2026, the first harmonized EU AI Act standard (cited in the Official Journal of the European Union in October 2026), maps to the Article 17 quality management system required of providers of high-risk AI systems. Most organizations using AI are deployers rather than providers; deployer-side AI-use governance is where the mappings in this guide apply.

WHY COMPLIANCE TEAMS CHOOSE SHADOW DEFEND

From Invisible to Auditable

For compliance and security teams, the challenge is not just detecting AI use. It is turning fragmented activity into evidence, policy action, and audit readiness. Shadow Defend helps teams move from reactive discovery to a more repeatable governance program.

Discover previously unknown AI usage across your organization	Build defensible, timestamped audit trails for assessments
Reduce data leakage risk from unsanctioned AI tools	Accelerate compliance assessments with ready evidence
Support AI governance initiatives aligned to ISO 42001	Improve vendor oversight and third-party risk management

See how Shadow Defend supports AI compliance readiness

Schedule a demo or request a tailored compliance mapping review to see how Shadow Defend can help your organization identify browser-based AI usage, strengthen controls, and prepare for audits with greater confidence.

shadowdefend.com/demo

Built for enterprise security, compliance, and AI governance leaders.

