stackArmor

A TYTO ATHENE COMPANY

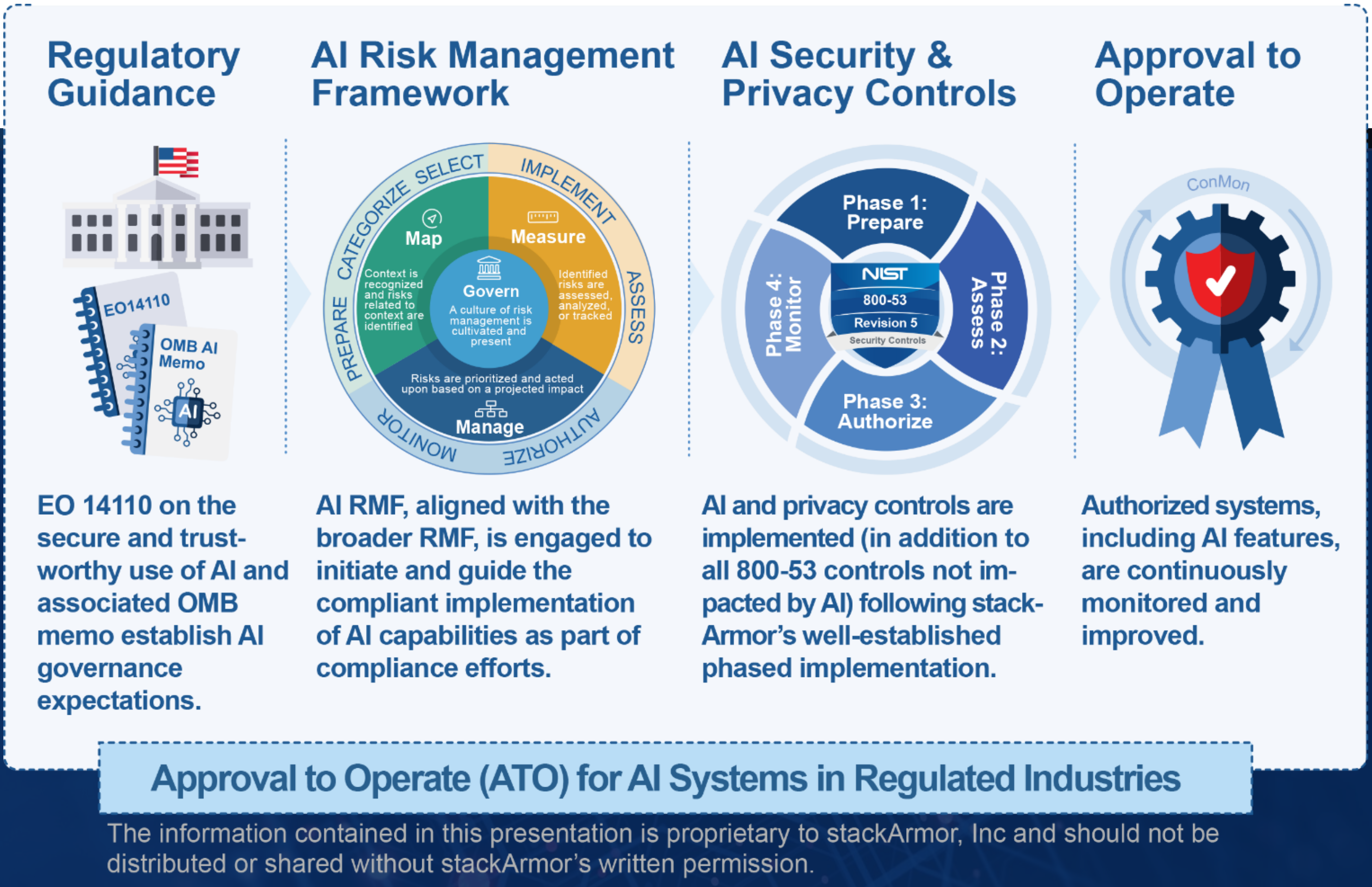
Assessing and Accrediting AI Systems

Extending Cyber Risk Management to include Safety Risk Management by applying NIST SP 800-53 Security Controls with AI specific Control Overlays presents an accelerated pathway for assessing and accredited AI systems within the Public Sector.

The **Whitehouse Executive Order (EO 14110)** on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence directs Agency Chief Information Officers, Chief Information Security Officers, and authorizing officials to operationalize generative AI and other critical and emerging technologies. Agencies must incorporate risk management tailored to AI systems. The NIST AI Risk Management Framework (NIST AI 100-1) helps manage the many risks of AI and promote trustworthy and responsible development and use of AI systems. Given the stringent timelines associated with implementing strong governance and risk management protocols, agencies should consider augmenting and enhancing existing risk management models such NIST RMF and NIST SP 800-53 with AI specific Control Overlays to accredit AI systems.

Putting NIST AI RMF into Practice: Actionable Playbook

The gap between NIST AI RMF concepts and actionable guidance can be filled by mapping NIST AI RMF risk categories to NIST SP 800-53 controls and implementing an integrated governance model. The integrated governance model builds upon existing practices covering cybersecurity risk and is further expanded to include AI specific risks like bias, safety and explainability. By starting with NIST AI RMF risk categories mapped to NIST SP 800-53 controls with AI control overlays – then executing the NIST RMF activities - we get an actionable playbook for public sector AI systems assessment and accreditation. The following infographic shows the overall governance model.



Regulatory Guidance

EO 14110 on the secure and trustworthy use of AI and associated OMB memo establish AI governance expectations.

AI Risk Management Framework

PREPARE
CATEGORIZE
SELECT
IMPLEMENT
ASSESS
AUTHORIZE
MONITOR
Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Risks are prioritized and acted upon based on a projected impact
Manage

AI RMF, aligned with the broader RMF, is engaged to initiate and guide the compliant implementation of AI capabilities as part of compliance efforts.

AI Security & Privacy Controls

Phase 1: Prepare
Phase 2: Assess
Phase 3: Authorize
Phase 4: Monitor
NIST
800-53
Revision 5
Security Controls

AI and privacy controls are implemented (in addition to all 800-53 controls not impacted by AI) following stackArmor's well-established phased implementation.

Approval to Operate

Authorized systems, including AI features, are continuously monitored and improved.

Approval to Operate (ATO) for AI Systems in Regulated Industries

The information contained in this presentation is proprietary to stackArmor, Inc and should not be distributed or shared without stackArmor's written permission.

stackArmor's ATO for AITM Governance Model

We are an inaugural member of the NIST US Safety Institute Consortium. Our Security & Compliance experts help agencies implement an auditable AI Risk Management Program based on NIST AI RMF & AI Overlay Controls.

Visit us at https://stackarmor.com/ai/ to download our Free Whitepaper.