



Secure by Design in the Age of AI™

The Product Security Operating Model for the AI Era

Stephen R. Jordan

Volume VII of *The Operating Discipline for AI Library™*

Pillar II: AI Risk Governance & Security™

The product security operating model for the AI era. Engineering velocity has grown by an order of magnitude while security review capacity has not, and AI adds vulnerabilities at the meaning layer that deterministic tooling cannot reliably find. The book names that condition the Dual Impedance Problem and installs five frameworks that answer it. Written for CISOs, CTOs, and engineering and product leaders, Volume VII offers libraries a contemporary reference on secure software development in the AI era. Recommended for computer security, information technology, and business collections.

BIBLIOGRAPHIC

Title	Secure by Design in the Age of AI™
Author	Stephen R. Jordan
Publisher	SRJ Consulting & Services Publishing
Pub. Date	September 8, 2026
Pages	444

FORMATS & PRICING

Hardcover	ISBN 979-8-9969402-9-5 · \$109.99 USD
Paperback	ISBN 979-8-9969402-8-8 · \$46.99 USD

Order in hardcover and paperback editions through Amazon. For acquisition inquiries, contact the publisher directly.

WHAT IS INSIDE

- The AI Attack Surface Ledger**, one row for every boundary crossing in every product.
- The AI Feature Tier Map and the Seven Stop Conditions**, which decide where scarce human judgment goes.
- The Two Lane Assurance Model**, sending rate to the machine and kind to the human.
- The Ship Decision Record and the Product Security Case**, which produce release evidence rather than remediation evidence.
- The Review Capacity Ratio**, turning a backlog complaint into a decision a CFO can act on.

ABOUT THE AUTHOR

Stephen R. Jordan is the founder of SRJ Consulting & Services LLC, an operator led AI advisory practice serving mid market to multinational organizations. His career spans senior roles at Citi, Intel, McAfee, and Optiv across technology operations, security, and enterprise risk. He is the author of *The Operating Discipline for AI Library™*, a nine volume executive reference series organized into two pillars, AI Business Services™ (Volumes I through IV) and AI Risk Governance & Security™ (Volumes V through IX), all nine now published. Based in Frisco, Texas. Works nationwide.

LIBRARY APPEAL

Public libraries: A strong fit for technology and career sections serving IT and security professionals, and for business readers who need to understand AI risk without a technical background. **Academic libraries:** Recommended for cybersecurity, computer science, and information systems programs, and for business schools teaching technology risk. Aligned with the CISA Secure by Design program, OWASP LLM Top 10, and NIST SSDF, and suitable for course adoption in software security, secure software engineering, and product management. **Corporate and special libraries:** Useful for security, risk, and compliance teams preparing for AI audits, customer security reviews, and regulatory inquiries.

PUBLISHER CONTACT

SRJ Consulting & Services Publishing
Frisco, Texas, USA

EMAIL

info@srjconsultingservices.com

PHONE

(415) 413-7772

WEB

srjconsultingservices.com