Adam G. Hopkins, CISSP, AIGP

Summary

Adam G. Hopkins is a highly experienced cybersecurity, AI governance, compliance automation, and enterprise security architecture leader with more than 20 years of progressive experience across IT governance, AI risk management, control framework development, M&A security due diligence, third-party risk management, audit readiness, and enterprise security operations. His experience developing and operationalizing Oracle's AI Security Framework, combined with his practical automation capability and framework-based risk methodology, makes him exceptionally well qualified to support organizations seeking to understand and improve their cybersecurity, digital governance, and AI governance posture.

Adam brings the ability to assess cybersecurity and AI governance programs from both a technical and executive perspective. He can evaluate AI control maturity, security architecture, compliance alignment, vendor risk, M&A integration risk, IT general controls, evidence quality, and operational readiness, while also translating findings into business-focused recommendations that leadership can act on. His depth of experience, professional credentials, and practical assessment background make him a strong asset for cybersecurity consulting, audit support, AI governance reviews, acquisition diligence, third-party reviews, and enterprise risk advisory engagements.

Professional Cybersecurity Assessment Bio

Adam G. Hopkins is a senior security and trust leader with more than two decades of experience designing, securing, evaluating, automating, and improving complex technology and compliance environments across enterprise technology, cloud, manufacturing, acquisition, and regulated operating models. His career reflects a strong progression from hands-on IT systems, security operations, and architecture roles into director-level leadership across AI governance, M&A security, compliance automation, IT controls, third-party risk management, and enterprise cybersecurity risk evaluation.

Adam brings a rare combination of deep technical knowledge, AI governance experience, executive risk insight, and practical automation capability. He has spent much of his career helping organizations understand security posture, identify control gaps, evaluate technical and operational risk, improve audit readiness, and translate complex findings into clear, actionable recommendations for leadership teams. His background makes him especially valuable in cybersecurity assessment, AI governance review, compliance automation, audit readiness, security due diligence, and risk-based advisory engagements.

AI Governance and Emerging Technology Risk Leadership

At Oracle, Adam serves as Director of Security, M&A and AI Risk Management, where he provides strategic security and trust leadership for AI security governance, compliance program management, audit coordination, and acquisition integration security. In this role, he partnered with information security, legal, and AI data science teams to develop and operationalize Oracle's AI Security Framework, including AI asset inventory management, automated model card generation, risk assessments, and pre- and post-deployment monitoring aligned to ISO 42001, the EU AI Act, and NIST requirements.

Adam's AI governance work includes model review processes, training data protection standards, inference system monitoring protocols, lifecycle security expectations, and risk management practices for AI/ML in regulated environments. This experience allows him to assess whether AI systems are governed before deployment, monitored after deployment, and supported by control evidence throughout the AI lifecycle.

He has also conducted SOC 2 report reviews and vendor risk assessments for major AI platform providers, including OpenAI, xAI, Microsoft, and Cohere. This gives him direct experience evaluating third-party AI platform risk, provider assurance, data protection expectations, model governance, and customer trust considerations associated with enterprise AI adoption.

Adam's AI governance value extends beyond policy review. He has designed agentic AI-driven workflows to automate vendor security assessments and enable continuous risk monitoring. He has also built Python-based automation using AI coding tools, including Claude Code and Codex, to streamline third-party risk management, evidence collection, and compliance operations.

Cybersecurity Assessment and Risk Leadership

Adam has extensive experience leading and supporting cybersecurity assessments across enterprise environments, acquisition targets, vendors, cloud services, infrastructure, applications, and regulated control areas. At Oracle, he served as the primary security contact for security review engagements across more than 15 acquisition due diligence processes, coordinating control documentation, evidence collection, audit readiness, architecture reviews, compliance assessments, remediation tracking, and corrective action planning.

His assessment work has supported ISO 27001, HITRUST, SOC 2, SOX, ITGC, vendor governance, cloud security, and AI governance requirements. Adam has evaluated environments ranging from smaller acquisition targets to complex global transactions, including the Cerner acquisition, where control maturity, integration risk, regulatory alignment, and long-term remediation planning were critical to successful security integration.

Adam's assessment approach is structured, reusable, and evidence-based. He has cross-mapped M&A risk assessment questions to NIST 800-53, ISO 27001, and ISO 42001 to

create reusable evidence sets and reduce duplicated assessment effort. This common control approach allows him to evaluate environments in a defensible manner while improving assessment consistency across concurrent compliance and audit workstreams.

M&A Security Due Diligence and Third-Party Risk Management

Adam brings deep experience in M&A security due diligence, acquisition integration, and third-party risk management. His work includes security reviews for more than 15 acquisitions, with responsibility for architecture reviews, compliance assessments, post-close remediation, long-term corrective action tracking, and coordination across corporate development, legal, privacy, product security, business units, and technical stakeholders.

His third-party risk work includes evaluating OneTrust for enterprise TPRM and vendor risk tiering, establishing inherent and residual risk scoring methodology, using JIRA for security findings and remediation tracking, and designing AI-enabled workflows to improve vendor assessment throughput and continuous risk visibility. This experience is especially valuable for organizations that rely on vendors, SaaS providers, cloud platforms, AI platforms, managed service providers, outsourced operations, and acquired technology environments.

Adam understands how third-party weaknesses can introduce enterprise risk and how to evaluate those risks using a practical, control-based assessment methodology. His ability to assess both internal and external environments makes him well suited for cybersecurity consulting engagements involving vendor assessments, acquisition diligence, enterprise security reviews, audit preparation, AI provider reviews, control maturity evaluations, and remediation planning.

Compliance Automation and Control Framework Alignment

Adam has strong experience modernizing compliance programs by moving organizations from manual evidence collection toward reusable controls, automation, and continuous monitoring. He has designed automated control frameworks, cross-mapped controls across multiple regulatory standards, and built dashboards that provide leadership with real-time visibility into audit readiness, vendor risk posture, AI program health, integration performance, and remediation progress.

His framework experience includes NIST 800-53, ISO 27001, ISO 42001, EU AI Act alignment, HITRUST, SOC 2, SOX, ITGCs, cloud security controls, vendor governance requirements, and AI lifecycle security expectations. This allows him to evaluate control environments in a structured and defensible manner while identifying opportunities to reduce duplication, improve evidence quality, strengthen governance maturity, and accelerate audit response.

Adam has also developed automation to standardize responses to client security questionnaires, audits, and RFPs, including a CIAQ automation template designed to improve

consistency and reduce manual effort. His experience connecting GRC processes, AI-enabled automation, evidence management, and executive reporting gives him a practical perspective on how organizations can mature from point-in-time compliance toward continuous assurance.

Security Architecture, IT Controls, and Operational Resilience

Adam's cybersecurity assessment background is grounded in strong technical capability. As Enterprise Security Architect at Adient, he executed ITGC compliance activities including access reviews, least privilege validation, and segregation of duties across enterprise systems in a global manufacturing organization with more than 230 facilities. He also served on the Global IT Security Governance Council, contributing to enterprise security policy development and risk acceptance processes across international business units.

His technical leadership includes cloud security architecture and advisory for Azure, Microsoft 365, MFA, DLP, and MDM, as well as the development of security baseline standards that supported cloud adoption without creating unnecessary operational bottlenecks. He designed and deployed a global vulnerability management program assessing more than 81,000 scanned assets and discovering more than 616,000 net-new assets, significantly improving enterprise risk visibility.

Earlier in his career, Adam managed security operations program delivery, SIEM deployment, IDS integration, forensic collection, deception technology, threat intelligence feeds, repeatable incident response processes, vulnerability management, application security integration, and policy development. This combination of technical assessment experience and enterprise risk leadership allows Adam to evaluate environments beyond policy-level review and validate whether controls are operating effectively.

Executive Communication and Actionable Recommendations

One of Adam's core strengths is his ability to communicate complex cybersecurity, AI governance, compliance, and technical findings to diverse audiences. He is experienced in working with information security, legal, privacy, data science, product security, corporate development, business units, auditors, risk management teams, and senior leadership to ensure that assessment results are not simply documented but clearly understood and acted upon.

In cybersecurity and digital governance assessment work, this ability is critical. Technical findings must be prioritized, contextualized, and converted into business-focused recommendations. Adam can explain AI governance risk, audit readiness gaps, third-party exposure, control maturity, remediation priorities, and compliance automation opportunities in practical terms that support leadership decisions around investment, mitigation, risk acceptance, and operational change.

His leadership style is grounded in collaboration, technical credibility, and a strong understanding of enterprise risk. He is comfortable working with technical teams on detailed findings while also providing senior stakeholders with clear summaries, risk themes, dashboards, and strategic recommendations.

Professional Credentials

Adam holds a Master of Science in Cyber & Information Security from Capitol Technology University and a Bachelor of Science in Information Systems Security with a concentration in Cloud Computing from American Public University.

His professional credentials include CISSP and AIGP, reflecting a strong foundation across cybersecurity governance, enterprise risk management, security architecture, and artificial intelligence governance. He has also completed CISM and CRISC coursework and maintains additional professional development in ITIL, Kepner-Tregoe, and leadership development programs.

His certifications, combined with decades of hands-on and leadership experience, position him as a trusted cybersecurity assessment professional capable of evaluating complex environments, identifying material risk, strengthening AI governance, improving compliance automation, and providing practical guidance aligned to business needs and recognized industry standards.