Anthony M. Bisulca IV, CISSP, GPEN, GSNA, CCSP, InfoSEC

Summary

Anthony M. Bisulca IV is a U.S. Army veteran, senior cybersecurity executive, CISO, and global cybersecurity assessment leader with more than 21 years of experience building, leading, and maturing cybersecurity, compliance, security operations, third-party risk, vendor risk, and global assessment programs across Fortune 100, Fortune 500, startup, SaaS, payment, manufacturing, offshore development, call center, and highly regulated environments. His background includes senior cybersecurity leadership roles with Apple, Oracle, BEA Systems, and Procare Solutions, where he has led enterprise-scale security initiatives, global cybersecurity assessments, M&A security reviews, vendor due diligence, compliance programs, product security, incident response, and executive risk reporting.

Anthony brings a rare combination of hands-on cybersecurity engineering depth, global assessment leadership, CISO-level accountability, business risk alignment, and practical execution experience. He has created and led multiple global cybersecurity assessment teams and programs across Apple, Oracle, and BEA Systems, including programs focused on **Mergers & Acquisitions, Third-Party Risk, Vendor Risk, Call Centers, Recycle Centers, Offshore Development Centers, Contract Manufacturing Locations, SaaS platforms, payment environments, and global enterprise operations**.

Cybersecurity Assessment and Risk Leadership

Anthony has built and led cybersecurity assessment programs across some of the world's most complex technology and operational environments. His assessment leadership includes global third-party security assessments, vendor risk reviews, acquisition security assessments, manufacturing security evaluations, offshore development center assessments, call center security reviews, recycle center security evaluations, cloud and SaaS security reviews, product security assessments, and operational risk evaluations.

At Apple, Anthony built and managed a domestic and global third-party security assessment program supporting more than **24,000 critical (Single Point of Failure) vendors**, significantly strengthening supply chain visibility and reducing third-party cybersecurity exposure. His work included security reviews, risk assessments, vendor due diligence, and control evaluations across diverse technology, business, manufacturing, and operational environments.

Anthony's global assessment work has included international security deployment and planning efforts, including secure server room and infrastructure buildouts at contract manufacturing locations across multiple foreign countries. His experience assessing and securing global operational environments gives him direct insight into complex multinational, multi-stakeholder organizations.

At Oracle, Anthony served as a Senior Manager for Corporate Security Global M&A and Senior Principal Security Engineer, where he conducted security assessments for acquisition targets, inherited environments, applications, infrastructure, vendors, and business operations. He supported global M&A security integration by identifying security gaps, assessing operational risk, and aligning acquired environments to enterprise security standards.

At BEA Systems, Anthony managed security operations across **35 locations**, supporting monitoring, incident response, vulnerability management, access control, operational security, compliance, audit, customer security requirements, and control validation.

Global Security Assessment Program Development

Anthony has repeatedly built cybersecurity assessment functions from the ground up and scaled them into structured, repeatable, and business-aligned programs. His experience includes creating assessment methodologies, defining control expectations, leading distributed teams, coordinating with technical and non-technical stakeholders, and translating technical risk into practical remediation plans.

Across Apple, Oracle, BEA, and Procare Solutions, Anthony has assessed environments involving corporate infrastructure, vendor ecosystems, acquired companies, SaaS applications, payment systems, manufacturing environments, offshore development centers, call centers, recycle centers, and third-party service providers. This breadth allows him to evaluate cybersecurity risk holistically across people, process, technology, governance, and operational dependencies.

His assessment approach is grounded in practical evidence review, technical validation, risk prioritization, and executive communication. He understands that cybersecurity assessments must do more than identify deficiencies; they must help organizations make informed decisions, prioritize investments, strengthen governance, and reduce risk in a measurable way.

Anthony has also supported M&A security integration, acquisition security reviews, vendor due diligence, and inherited platform risk normalization, giving him extensive experience evaluating environments that may have inconsistent controls, fragmented ownership, legacy systems, varying maturity levels, and complex integration requirements.

CISO-Level Cybersecurity, Compliance, and Digital Governance Leadership

As the functional CISO for Procare Solutions, Anthony led cybersecurity, compliance, privacy, risk management, product security, security operations, vulnerability management, and enterprise governance across a multi-product SaaS portfolio supporting childcare management, payment processing, sensitive customer data, child data, PII, and PCI/payment information.

When Anthony joined Procare, he was the only dedicated cybersecurity resource. He built the cybersecurity organization into a five-person full-time and one part-time team focused on Compliance & Privacy, Security Operations, Vulnerability Detection & Management, and Cybersecurity Engineering.

He built and matured cybersecurity and compliance programs across **six SOC 2 Type II SaaS platforms** and **one PCI-DSS Level 1 payment processing environment**. These programs supported regulatory alignment, customer trust, audit readiness, security maturity, business growth, and operational resilience.

Anthony's compliance and governance leadership includes SOC 2 Type II, PCI-DSS 3.2.1 and 4.0.1, TX-RAMP, GDPR, CCPA, COPPA, FERPA, HIPAA, NIST CSF, NIST 800-53, ISO 27001, CIS Controls, COBIT, risk registers, audit readiness, control mapping, and evidence management.

Anthony has proven experience assessing cybersecurity maturity, reviewing governance structures, evaluating control environments, improving audit readiness, aligning security practices to recognized frameworks, and helping leadership understand risk in a clear and actionable way.

Third-Party Risk, Vendor Risk, and Supply Chain Security

Anthony has deep expertise in third-party risk management, vendor risk, supplier security, and global supply chain cybersecurity assessment. His experience includes building and leading assessment programs that evaluate vendors, suppliers, service providers, outsourced development teams, manufacturing partners, call centers, recycle centers, and international operational sites.

At Apple, Anthony led a domestic and global third-party security assessment program supporting more than 24,000 critical vendors across multiple regions and business functions. This work strengthened supply chain security, improved vendor risk visibility, and helped the organization better understand cybersecurity exposure across an extensive third-party ecosystem.

His third-party risk experience includes security questionnaires, onsite reviews, vendor due diligence, control validation, risk scoring, remediation tracking, executive reporting, and business-aligned decision support. He has used and managed third-party risk tools including RiskRecon, BitSight, and HackNotice, and has experience integrating vendor findings into broader risk management and leadership reporting processes.

This experience is especially valuable for international organizations that depend on global vendors, outsourced service providers, regional partners, development teams, cloud platforms, and managed technology services. Anthony understands how to identify third-party risk, evaluate control maturity, prioritize remediation, and communicate risk in a way that supports governance and operational decision-making.

Product Security, Cloud Security, and Vulnerability Management

Anthony has led product security, cloud security, secure SDLC, DevSecOps, application security, vulnerability management, and engineering remediation programs across enterprise and SaaS environments. He has implemented secure development practices across multiple product teams using Veracode Static Application Security Testing, Contrast Security, Qualys, CrowdStrike, and Jira-integrated remediation workflows.

At Procare Solutions, Anthony established product-embedded security workflows where findings from code scanning, environmental scanning, cloud monitoring, endpoint detection, and compliance reviews generated Jira tickets assigned directly to development teams. He also created and maintained an enterprise risk registry and dashboard to track vulnerability findings, audit risks, remediation ownership, business impact, and leadership visibility.

Anthony’s technical and governance experience allows him to assess cybersecurity programs from both strategic and operational perspectives. He can evaluate whether vulnerabilities are being identified, whether remediation ownership is clear, whether risk is being tracked effectively, whether evidence exists to support audit conclusions, and whether executive leadership has meaningful visibility into the organization’s cyber risk posture.

His platform experience includes CrowdStrike Falcon Complete, CrowdStrike AI-DR, CrowdStrike Identity Protection, CrowdStrike Cloud, CrowdStrike SIEM, Abnormal.ai, Qualys, Veracode, Contrast Security, SafeBase, KnowBe4 KCM GRC, Carbide GRC, Archer, SharePoint evidence repositories, RiskRecon, BitSight, HackNotice, AWS, Azure, Microsoft 365, Jira, and CI/CD security workflows.

Incident Response, Threat Detection, and Operational Resilience

Anthony has built and led cybersecurity incident response programs across complex SaaS and enterprise environments. At Procare Solutions, he built the cybersecurity incident response program across a multi-product SaaS environment supporting sensitive customer, child, PII, and PCI/payment data. His incident response processes covered event triage, escalation, containment, eradication, recovery, executive communication, customer impact analysis, post-incident review, evidence retention, and corrective action tracking.

He integrated incident response workflows with modern detection and response platforms including CrowdStrike Falcon Complete, CrowdStrike Identity Protection, CrowdStrike Cloud, CrowdStrike SIEM, Abnormal.ai, Qualys, and Jira. He also established escalation paths for endpoint threats, identity compromise, phishing, account takeover, cloud risk, application vulnerabilities, vendor risk, and potential data exposure.

Anthony's operational resilience experience is directly relevant to cybersecurity audits because incident response maturity, monitoring capability, escalation discipline, remediation tracking, and evidence retention are critical indicators of whether an organization can detect, respond to, and recover from cyber events.

AI Security and Emerging Technology Governance

Anthony is a forward-looking cybersecurity leader with direct experience building AI security governance, AI risk management, AI monitoring, AI-DLC adoption, AI enforcement, sensitive data protection, and DLP considerations across engineering, product, finance, support, and executive users.

He has implemented governance and monitoring controls for generative AI adoption, helping organizations benefit from emerging technology while protecting sensitive data and reducing operational, privacy, and compliance risk. His experience with CrowdStrike AI-DR, AI monitoring, AI data protection, prompt injection risk, sensitive data leakage controls, and secure AI adoption provides an important perspective for digital governance engagements.

Anthony's AI governance experience adds valuable depth to digital governance engagements. Digital governance is no longer limited to traditional IT controls; it must also consider responsible adoption of emerging technologies, data protection, monitoring, user behavior, third-party platforms, and governance structures that support safe innovation.

Executive Communication and Board-Level Advisory

Anthony is a trusted advisor to executive leadership and Boards of Directors. He has presented cybersecurity strategy, enterprise risk posture, security maturity, compliance status, incident response readiness, investment priorities, and NIST CSF maturity reporting to executive teams and Boards.

He is highly effective at translating complex cybersecurity, regulatory, technical, and operational risk into business-aligned recommendations. His executive communication experience includes security roadmap development, cybersecurity budget planning, tooling prioritization, risk-based investment decisions, compliance readiness, audit status, customer trust, incident response reporting, and digital governance alignment.

This ability is critical for complex cybersecurity and digital governance audits. A successful cybersecurity and digital governance audit must produce findings and recommendations that are technically accurate, strategically meaningful, and understandable to senior stakeholders. Anthony's experience ensures that assessment results can be converted into actionable priorities, measurable improvements, and leadership-ready reporting.

Professional Credentials and Leadership Foundation

Anthony holds a Bachelor of Science in Computer Science from Metropolitan State College of Denver. His professional certifications include CISSP, CCSI, GPEN, GSNA, CCSP, CCDP, CCNP, ICI, MCSE, MCT and Infosec credentials.

In addition to his corporate cybersecurity career, Anthony is a U.S. Army veteran and former E-5 Squad Leader with the 2/504 Parachute Infantry Regiment, 82nd Airborne Division. His deployments included Sinai, Egypt; Honduras; and Panama. This experience helped shape his leadership approach around discipline, accountability, mission focus, risk assessment, communications, and execution under pressure.

Cybersecurity & Digital Governance Qualifications

Anthony's experience directly maps to the work required for serious cybersecurity and digital governance assessments, including:

Cybersecurity assessment leadership across global organizations, acquired companies, third parties, vendors, offshore development locations, call centers, recycle centers, contract manufacturing sites, SaaS platforms, and payment environments.

Governance, risk, and compliance experience across SOC 2, PCI-DSS, TX-RAMP, GDPR, CCPA, COPPA, FERPA, HIPAA, NIST CSF, NIST 800-53, ISO 27001, CIS Controls, COBIT, audit readiness, control mapping, and executive risk reporting.

Third-party and supply chain risk leadership, including global vendor security assessment programs supporting more than 24,000 critical vendors.

Hands-on product security, cloud security, application security, vulnerability management, incident response, threat detection, AI governance, and data protection experience.

Executive and Board-level reporting experience with a proven ability to translate technical findings into business, operational, governance, and investment decisions.

Anthony's background demonstrates that he has not only participated in cybersecurity programs — he has built them, led them, assessed them, remediated them, and presented their risks and outcomes to senior leadership. He brings the depth, credibility, and execution discipline required to perform meaningful cybersecurity and digital governance audits.

Anthony Bisulca is a principal cybersecurity assessment leader with the global experience, technical foundation, governance knowledge, and executive communication skills needed to evaluate cybersecurity maturity, identify material risks, strengthen digital governance, and improve organizational cyber resilience.