Dara F. Thomas

GRC Analyst | Security+ | CGE-AUD | ISO 27001 Lead Auditor | SOC 2, ISO 27001, Third-Party Risk

Atlanta, GA | dara.thomas.grc@gmail.com | linkedin.com/in/darafthomas | github.com/DaraStaysCurious

SUMMARY

GRC analyst with 10+ years of risk, audit, and corrective-action experience in highly regulated manufacturing, maritime, and offshore energy environments, plus 6 years of UX research into how people work in B2B SaaS. The through-line is risk methodology: ISO 19011 audit practice (the basis for ISO 27001 internal audits under ISO/IEC 27007), root cause analysis, and corrective-action tracking, now applied to SOC 2, ISO 27001, NIST CSF 2.0, HIPAA, and PCI DSS readiness through case-study compliance programs. UX research adds a human-risk lens on why controls get bypassed under deadline pressure. Designs controls that pass audit and hold up in real use.

CERTIFICATIONS

CompTIA Security+ | Certified GRC Engineer - Auditor (CGE-AUD) | MasterMind ISO 27001 Lead Auditor | AWS Certified Cloud Practitioner (in progress)

AREAS OF EXPERTISE

- **Frameworks & Standards:** SOC 2 Type II, ISO 27001:2022, NIST CSF 2.0, HIPAA Security Rule, PCI DSS v4.0, NIST SP 800-30
- **Risk & Compliance:** Third-party/vendor risk management (attestation review, monitoring plans), risk assessment and risk register management, audit readiness and evidence collection, control mapping and gap analysis, policy and procedure development, compliance documentation
- **Methods & Tools:** ISO 19011 internal audit methodology (basis for ISO 27001 audits via ISO/IEC 27007), root cause analysis (Five Whys), corrective-action tracking, Fine-Kinney risk scoring with a NIST SP 800-30 crosswalk, GRC data modeling (ServiceNow App Engine Studio), process mapping and stakeholder interviews
- **Human Risk & Control Design:** User research methods (stakeholder interviews, usability testing, workflow mapping) applied to predicting control bypass and designing controls for actual use; see TrustPath case study.
- **Communication & Collaboration:** Stakeholder alignment, communicating risk to leadership, facilitation, training

KEY ACHIEVEMENTS

- **Gap Analysis & Control Mapping:** Assessed 41 applicable ISO 27001:2022 Annex A controls for a case-study workforce safety SaaS platform handling employee health records, identifying 33 critical and high-severity gaps and mapping them to HIPAA and NIST CSF 2.0.
- **Third-Party Risk Assessment:** Assessed three HRIS vendor integrations (Workday, ADP, BambooHR) by reviewing public SOC 2 and ISO attestations; flagged ADP's limited ISO certificate scope and BambooHR's unconfirmed ISO 27001 claim, rated residual risk, and set a monitoring plan with 12-month reassessment.
- **Audit Remediation:** Closed 100% of validated findings from comprehensive Process Safety Management audits, typically 25-40+ complex findings per audit, within 30-90-day corrective action tracking windows.
- **Regulatory Compliance:** Owned safety and regulatory risk governance for a 270-employee manufacturing plant, achieving 14 consecutive quarters without a major regulatory citation.
- **Policy & Procedure Development:** Managed the policy lifecycle for an incident response plan and 8 critical task procedures at Unilever Bramalea; authored or revised 15 critical task procedures at Tucker Energy.
- **Cross-Functional Remediation:** Translated risk and process-gap findings into remediation plans with product and engineering teams across 15+ B2B SaaS engagements, reducing user-reported errors by an estimated 35%.

PRACTICAL GRC PROJECTS (SELF-DIRECTED)

Five self-directed projects covering SOC 2, ISO 27001, NIST CSF 2.0, PCI DSS v4.0, and NIST SP 800-30.

- **OccuSafe - ISO 27001 / HIPAA / NIST CSF 2.0 (case study):** ISO 27001:2022 gap analysis, HRIS vendor risk assessment, and a linked Policy-Control-Risk data model in ServiceNow App Engine Studio.
- **Carestream - SOC 2 Type II / HIPAA Audit Readiness (case study):** Built a SOC 2 Type II readiness assessment for a healthcare SaaS company across the Security, Availability, Confidentiality, and Privacy criteria; produced a HIPAA-to-SOC 2 crosswalk, a NIST SP 800-30 risk assessment, and a prioritized remediation roadmap for 4 critical findings (offboarding, session management, third-party EHR integration risk, security awareness training).
- **TrustPath - Usable Security (case study):** Assessed a B2B SaaS vendor risk platform against SOC 2 and NIST CSF, paired with a human-risk assessment using UX research methods to explain why controls get bypassed under deadline pressure.

- **PayGuard - PCI DSS v4.0 Readiness Assessment (case study):** Assessed all 12 PCI DSS v4.0 requirements for a payment processor approaching Level 1 status, with NIST SP 800-30 risk scoring, a CDE segmentation review, and a prioritized remediation roadmap.
- **Risk Methodology - Fine-Kinney × NIST SP 800-30:** Built a crosswalk between Fine-Kinney risk scoring and NIST SP 800-30, proposing Exposure as an explicit risk-model variable; applied it to three OHS incident case studies.
- View all projects here - Portfolio: darasecures.cloud | GitHub: github.com/DaraStaysCurious

PROFESSIONAL EXPERIENCE

Independent Consultant, Self-Employed | *Remote* | *01/2020 - Present*

- Conducted risk assessments and stakeholder audits across 15+ B2B SaaS client engagements, applying Fine-Kinney risk scoring and Five Whys root cause analysis to surface workflow and control gaps.
- Delivered client risk reports (risk identification, likelihood and impact, inherent and residual ratings, treatment and ownership recommendations) and IT risk registers, and completed vendor security questionnaires.
- Partnered with product and engineering teams to turn process-gap findings into prioritized remediation plans; presented findings to client leadership and formalized the method into a repeatable gap-analysis framework.
- Completed SOC 2 Type II, ISO 27001:2022, PCI DSS v4.0, and HIPAA readiness assessments for case-study SaaS companies (see Practical GRC Projects), using NIST SP 800-30 risk scoring and prioritized remediation roadmaps.

Sr. UX Designer, Child Care Aware of America | *Arlington, VA (Remote)* | *11/2023 - 02/2025*

- Designed and launched a voucher portal handling sensitive family data, now used by 15,000+ military families and replacing 7 hours of manual processing weekly.
- Surfaced 4 critical workflow risks pre-launch via usability testing and stakeholder interviews, enabling early remediation.
- Ran process analysis and risk reviews across 7 major features, documenting control-relevant changes for audit readiness.

Associate UI/UX Designer, Point B | *Portland, OR (Remote)* | *08/2021 - 10/2022*

- Facilitated workflow mapping workshops with 8 cross-functional teams to prioritize remediation on a training platform.
- Cut support requests by an estimated 27% and lifted completion rates by redesigning flows around risk findings.

Operations & Coordination Roles | *San Diego, CA and Atlanta, GA* | *03/2017 - 03/2020*

- Brinks Plumbing Services (vendor coordination, accounts payable); United Way of San Diego County (80+ stakeholder interviews, 100+ program assessments); Robert Half Agency (60+ client shipment issues resolved weekly across 15 dispatchers). Common thread: stakeholder interviewing.

Career Break - International Relocation, Canada to U.S. (09/2015 - 03/2017): professional development for career transition.

Occupational Health, Safety & Risk Manager, Unilever Bramalea | *Toronto, Canada* | *10/2008 - 09/2015*

- Reduced monthly incident investigations from 3 to 1 at a 270-employee edibles plant through risk-based hazard controls.
- Managed the policy lifecycle for the incident response plan and 8 critical task procedures, including a hoist fall-hazard redesign (4-strap tote bags) that reduced bag failures and fall risk.
- Audited to ISO 14001 and OHSAS 18001 (now ISO 45001) using ISO 19011, the basis for ISO 27001 audits.

Occupational Health, Safety & Risk Manager, Unilever Caribbean | *Trinidad, W.I.* | *08/2004 - 10/2008*

- Directed safety and compliance across 2 plants (edibles, 20 employees; detergents, 35), running twice-daily walkabouts, weekly safety meetings, and quarterly audits.
- Led comprehensive Process Safety Management audits, tracking corrective actions to closure within 30-90 days.
- Reduced safety incidents by an estimated 33% by remediating two root causes: installing non-removable machine guards, and floor resurfacing paired with more frequent cleaning.

Occupational Health, Safety & Risk Manager, Tucker Energy Services | *Offshore Oil Rigs, Trinidad, W.I.* | *08/2003 - 08/2004*

- Conducted monthly HSE and Process Safety Management audits across 2 oil rigs, plus quarterly cross-functional audits with supervisors and union reps.
- Authored or revised 15 critical task procedures; delivered monthly safety training to ~110 employees across both sites.

Health, Safety & Risk Manager, Royal Caribbean | *Radiance of the Seas, Brilliance of the Seas* | *07/2000 - 08/2003*

- Reduced incident investigations from 7-8 to 2 per 6-month cycle across 2 cruise vessels through root cause analysis.
- Led a 20-person emergency response team, improving response time by 10%; twice named Employee of the Quarter.

COMMUNITY & PROFESSIONAL ENGAGEMENT

Director of Membership (Volunteer), GRC Engineering Club - Atlanta Chapter | *Atlanta, GA* | *08/2026 - Present*

EDUCATION

University of Toronto, Canada - Honors B.A. Sociology and Equity Studies