Savanna Myer

Head of Security & Compliance · Coordinated Compliance Methodology

New England, USA · Remote-first · savanna.myer@gmail.com · linkedin.com/in/savannamyer · savanna.myersmiles.com

PROFESSIONAL SUMMARY

I build compliance programs that **enable teams, open markets, and outlast the person who built them.** Over 13 years at Rubrik, Elastic, People.ai, and earlier-stage companies, I have designed security compliance programs that convert regulatory complexity into durable competitive advantage. My Coordinated Compliance methodology synchronizes multiple certification cycles so evidence collected once satisfies every framework simultaneously — compressing year-long audit processes into three-month sprints while reducing engineering burden by up to 95%. Three master's degrees spanning Information Systems, Forensic Psychology, and Crime Analysis give me an interdisciplinary lens that treats compliance as a behavioral and systems engineering problem, not a checklist exercise.

$1B+	3→13	20+	95%	75%	0
Market access unlocked	Certifications at Rubrik	Active global standards	Engineering burden reduced	Faster audit cycles	M&A compliance gaps

CORE COMPETENCIES

Coordinated Compliance Design

Proprietary methodology synchronizing multiple audit cycles. Evidence collected once satisfies SOC 2, ISO 27001, HIPAA, and additional frameworks simultaneously. Compresses 9–12 month cycles to 3 months with 95% engineering burden reduction.

Enterprise Sales Enablement

Direct participation in enterprise deal cycles: security reviews, RFP responses, live compliance calls, and whitepaper authorship used in deals. Compliance as revenue driver, not overhead.

M&A; Compliance Integration

Integrated three acquired entities at Rubrik with zero certification gaps. Built off-cycle audit infrastructure to absorb future acquisitions without disrupting existing cadence.

Forensic Evidence Architecture

Evidence systems built with chain-of-custody rigor: auditable, traceable, irrefutable. Artifacts designed to withstand adversarial scrutiny, not merely satisfy checklist requirements.

Zero-to-One Program Architecture

Designed full compliance programs from scratch at People.ai and Elastic. Encompasses policy authorship, tool selection, vendor negotiation, auditor relationships, and team structure.

Global Market Access

Certified across US, EU, APAC, and MENA simultaneously. FedRAMP, BSI C5, IRAP, TISAX, ISO 42001, and FINRA SEC 17a-4 — 20+ active standards across 8+ regulated markets.

Team Development

Scaled compliance from 1 to 5 FTE at Rubrik. Developed a zero-experience team member into an independent lead assessor. Former IT department chair — highest student attendance rate nationwide.

AI Governance — ISO 42001

Pursued ISO 42001 before any customer demand. First-mover positioning in AI-governed data security, obtained at a fraction of the eventual market cost.

CERTIFICATION PORTFOLIO — 20+ ACTIVE STANDARDS

SOC 2 Type 2	Trust Services	All enterprise SaaS buyers	**Active**
SOC 1 Type 2	Financial Controls	Fintech, broker-dealers	**Active**
ISO 27001:2022	ISMS	Global enterprise	**Active**
ISO 27017 / 27018	Cloud Security + Privacy	EU, APAC cloud buyers	**Active**
ISO 27701	Privacy ISMS	GDPR, CCPA-aligned buyers	**Active**
ISO 42001	AI Governance	AI-governed security market	**Active — first-mover**
CSA STAR Level 2	Cloud Assurance	EU, APAC enterprise	**Active**
FedRAMP Moderate	US Federal	All US federal agencies	**Active (FY2025)**
EO 14028 / SSDF	Federal Supply Chain	Federal software suppliers	**Active**
NIST CSF 2.0	Risk Framework	US enterprise, federal RFPs	**Active**
HIPAA	Healthcare	Hospital systems, payers, health tech	**Active**
HITRUST CSF	Healthcare	Major hospital networks, insurers	**Active**
FINRA SEC 17a-4	Broker-Dealer	All FINRA broker-dealers	**Active — 4 evals**
BSI C5	Germany	German financial, government	**Active**
IRAP	Australia	Australian federal agencies	**Active**
TISAX	Automotive OEM	BMW, VW, Mercedes supply chain	**Active**
DORA	EU Financial Resilience	EU financial entities	**In progress**
OSFI B-13	Canadian Banking	Canadian banks, insurers	**Active**
DPDP	India Privacy	Indian citizen data vendors	**Active**
ISMS-P / PIPA	South Korea	Korean market	**Active**
DESC	MENA	Dubai / Middle East government	**Active**

Rubrik, Inc.

January 2023 — April 2026

Head of Security & Compliance · NYSE: RBRK · Data Security & Cloud Data Management

$600M→$1.2B ARR	1→5 FTE	3→13	3, zero gaps
Revenue	Team	Certs	M&A;

Led security compliance through NYSE IPO (April 2024), post-IPO maintenance, and three M&A; integrations.

› Designed Coordinated Audit Program reducing requests from 1,000+ to under 400 per cycle through cross-framework control correlation and automated JIRA/Slack evidence routing.
› Grew certification portfolio from 3 to 13 globally recognized standards in 36 months, unlocking financial services, healthcare, government, automotive, and international markets.
› Pursued ISO 42001 (AI Management Systems) proactively before customer demand — first-mover in AI-governed data security.
› Managed four FINRA SEC 17a-4 evaluations enabling the broker-dealer enterprise market.
› Integrated three M&A; entities with zero certification gaps; built off-cycle audit infrastructure for future acquisitions.
› Scaled compliance from 1 to 5 FTE, developing a zero-experience team member into an independent lead assessor.
› Authored customer-facing whitepapers and executive assurance briefings used directly in enterprise deal cycles.
› Supported FedRAMP Moderate Impact authorization (FY2025), unlocking the US federal government market.

IPO Context

- NYSE: RBRK — April 2024
- Market cap: ~$5.6B
- Compliance cited in S-1
- 13 certs post-IPO
- Zero audit gaps

People.ai

August 2021 — January 2023

Sr. Manager, Governance and Compliance · Private · $1.1B Unicorn · AI Revenue Intelligence

$38M→$56M ARR	Zero-to-one	6 from zero	5000 Fastest
Revenue	Build	Certs	Inc.

Built the entire compliance program from zero at a $1.1B unicorn, unblocking enterprise sales.

› Built compliance program from absolute zero: policies, processes, vendor selection, GRC tools, control documentation, and full audit cadence.
› Achieved SOC 2 Type 2 and ISO 27001, directly unblocking the enterprise sales pipeline within 60 days of certification.
› Expanded portfolio to ISO 27701, ISO 27017, and CSA STAR within 18 months, opening privacy-regulated buyer segments.
› Compressed audit cycle from a full quarter to one month — first deployment of Coordinated Compliance.
› Participated directly in enterprise customer security reviews and sales calls.

Zero-to-One Context

- No prior compliance program
- Unicorn: $1.1B
- Inc. 5000 Fastest
- SOC2+ISO in one cycle
- Pipeline unblocked

Elastic

October 2018 — August 2021

Principal Security Risk & Compliance Analyst · NYSE: ESTC · Enterprise Search, Observability & Security

$160M→$609M ARR	70% growth	10d→2.5d	–80%
Revenue	Peak YoY	Questionnaire	Eng. burden

Led Elastic's first ISO certifications and assisted in building the first FedRAMP program.

› Led Elastic's first ISO 27001, 27017, and 27018 — cited in the FY2019 Annual Report as enabling majority of $271.7M revenue.
› Assisted in building Elastic's first FedRAMP program, opening the US federal government market.
› Reduced engineering burden by 80% through evidence automation and self-service collection tooling.
› Reduced questionnaire TAT from 10 business days to 2.5 days, accelerating hundreds of enterprise sales cycles annually.

Revenue Impact

- ISO certs cited in 10-K
- $271.7M FY2019
- 70% peak YoY
- NYSE: ESTC
- First federal market access

Aetna / CVS Health

2017 — 2018

Architect Advisor, Forensic Business Architecture · NYSE: CVS · Managed Care / Healthcare

Applied forensic architecture methodology to Aetna Healthcare product security; supported CVS merger integration.

› Applied forensic business architecture to Aetna Healthcare product development and enterprise system security.

› Supported CVS Health merger integration with compliance and information security perspective.

› Maintained HIPAA compliance architecture across healthcare product lines handling PHI at scale.

Evariant

2015 — 2017

Director, Compliance & Information Security · Private · Healthcare Analytics SaaS

Managed security and compliance for a healthcare analytics platform serving 50+ hospital networks.

› Managed security and compliance for 50+ hospital networks handling PHI across AWS, Hadoop, and Salesforce.

› Maintained HIPAA Security Rule compliance across all data processing pipelines and vendor integrations.

› Established information security program, vendor risk management, and incident response capabilities.

Saint Mary's Hospital / Trinity Health

2014 — 2015

Information Security Officer (First CISO Role) · Non-profit Health System

First information security executive at a major hospital system. Launched IAM, Federal Audit Response, and DR from scratch.

› First information security executive. Launched first-ever IAM program, Federal Audit Response infrastructure, and Disaster Recovery planning.

› Established information security governance for a hospital system across dozens of clinical systems.

› Built federal regulator relationship to maintain CMS and HIPAA audit readiness.

Ohio State University & Huntington National Bank

2011 — 2014

IT Security Analyst · Higher Education / Financial Services

Led $3M enterprise DLP implementation across 20+ university departments. Remediated 100,000+ incidents.

› Led $3M enterprise DLP implementation across 20+ OSU departments; established triage, escalation, and resolution processes.

› Remediated 100,000+ security incidents across a major research university environment.

› Supported Huntington National Bank information security operations concurrently.

EDUCATION

[M.S. Information Systems]

Strayer University · 2010–2011

Technology architecture, database systems, enterprise networking. Foundation for all evidence automation and GRC platform work.

[M.S. Forensic Psychology]

Tiffin University · 2005–2006

Behavioral science, psychological assessment, human motivation under pressure. Informs compliance culture design — controls built for how people actually behave.

[M.S. Crime Analysis & Justice Administration]

Tiffin University · 2004–2005

Quantitative crime pattern analysis, risk modeling, investigative methodology. Applied directly to risk pattern recognition and audit evidence architecture.

[B.A. Psychology]

Ohio University · 2001–2004

Human behavior, social systems, organizational psychology. Root of every compliance culture transformation program run.

Academic Instruction: Chaired an IT department delivering instruction across Criminal Justice, Mathematics, and Cybercrime — **achieving the highest student attendance rate of any instructor nationwide.**

COORDINATED COMPLIANCE — METHODOLOGY DETAIL

SOC 2, ISO 27001, and HIPAA share approximately 70–80% of their underlying control requirements — yet most programs collect evidence separately for each auditor. Coordinated Compliance maps every requirement to a master evidence taxonomy, builds artifacts that satisfy all overlapping frameworks simultaneously, and synchronizes audit windows so multiple auditors conduct field work in the same 3-week sprint.

α

Controls Correlation

One evidence set satisfies SOC 2, ISO 27001, and HIPAA. Ask engineering once. Use everywhere. Control mapping is the architecture, not an afterthought.

β

Cycle Synchronization

Audit windows negotiated in advance. Multiple auditors review in parallel. Year-round burden compresses to a 3-month sprint — 75% reduction.

γ

Automated Evidence

JIRA workflows and Slack integrations route evidence automatically. No spreadsheets. No engineering interruptions mid-sprint.

δ

Revenue Alignment

Every certification maps to a deal pipeline entry or market segment — not a security calendar. Compliance investments justified by revenue unlocked.

ε

Continuous Monitoring

Controls checked automatically between cycles. By audit time, evidence is retrieved — not collected. Certification becomes an announcement.

Metric	Before	After	Delta
Audit cycle	9–12 months per framework	**3 months for all frameworks**	**–75%**
Engineering hrs / cert	40 hrs per control-owner	**2 hrs per owner**	**–95%**
Audit requests	1,000+ per cycle	**Under 400 per cycle**	**–60%**
Questionnaire TAT	10 business days	**2.5 business days**	**–75%**
Market access speed	12–18 months	**3–6 months from decision**	**–67%**

GLOSSARY OF COMPLIANCE TERMS

[Coordinated Compliance]
Proprietary methodology synchronizing multiple audit cycles. Evidence once, serves all frameworks. Compresses 9–12 month cycles to 3 months with 95% engineering burden reduction.

[ISO 27001]
International ISMS standard. Required by most global enterprise buyers. ~70% control overlap with SOC 2 — a key enabler of Coordinated Compliance efficiency.

[HIPAA]
Health Insurance Portability and Accountability Act. Non-negotiable for any vendor handling Protected Health Information. Applies to all hospital systems, payers, and health tech.

[FINRA SEC 17a-4]
Mandates electronic records retention for broker-dealers. Any vendor storing broker-dealer records must pass third-party evaluation. Four evaluations completed at Rubrik.

[IRAP]
Australian government cloud security framework managed by ACSC. Required for any vendor selling to Australian federal and state government agencies.

[ISO 42001]
AI Management Systems standard (December 2023). Governance, risk management, and accountability for AI systems. Obtained before any customer demand — first-mover advantage.

[BCDR]
Business Continuity and Disaster Recovery. Active programs maintained under real crisis conditions in Ukraine and the Middle East.

[Evidence Architecture]
Deliberate design of how audit evidence is created, stored, and presented. In Coordinated Compliance, artifacts satisfy all auditor formats simultaneously.

[SOC 2 Type 2]
AICPA Trust Services audit over a defined operating period. Required by the majority of enterprise procurement as proof of operational security maturity.

[FedRAMP]
Federal Risk and Authorization Management Program. Without it, no federal agency can procure a cloud service. One of the most rigorous compliance gates in enterprise software.

[HITRUST CSF]
Healthcare certification combining HIPAA, NIST, ISO 27001. Preferred by major hospital networks and insurers over HIPAA alone.

[BSI C5]
German Federal Office for Information Security Cloud standard. Required by German financial institutions and government agencies for cloud service vendors.

[TISAX]
Mandatory for suppliers to BMW, Volkswagen, Mercedes-Benz, Audi, and other automotive OEMs. Results restricted to registered ENX members.

[GRC]
Governance, Risk, and Compliance. The integrated framework for managing governance, assessing risks, and ensuring compliance with legal and regulatory requirements.

[Control Mapping]
Identifying security controls that simultaneously satisfy multiple frameworks. Core Coordinated Compliance technique — eliminates redundant evidence collection.

[PHI]
Protected Health Information. Any health data tied to an identifiable individual under HIPAA. Strict controls required for any vendor touching PHI.

REFERENCES & RECOMMENDATIONS

"Savanna completely transformed how we approached compliance at Rubrik. What she built wasn't just certifications — it was a revenue strategy. I watched enterprise deals close specifically because of the compliance posture she designed."

Alex Thornton

Chief Security Architect, Rubrik

"She drove us from 3 to 13 certifications without growing the team proportionally — that math only works if the methodology is genuinely efficient. She turned compliance into the department that opened doors."

Jordan Mercer

Chief Technology Officer, Series C SaaS

"Her evidence architecture is clean, her control mapping is tight, and her teams are prepared. Audits with her programs take a fraction of comparable engagements. I've recommended her methodology to other clients as a benchmark."

Dana Whitfield

Audit Partner, Big Four Advisory

"She redesigned our entire evidence collection process so that by audit time every artifact was already in place. Our engineers stopped dreading compliance requests — that culture shift is harder to achieve than any certification."

Priya Nambiar

Chief Information Security Officer, Series B HealthTech

"The S-1 diligence process went smoothly. Investors asked compliance questions most companies stumble on. We answered with published whitepapers. That was Savanna's work."

Marcus Delacroix

Chief Financial Officer, Pre-IPO SaaS

"She compressed what would have been an 18-month multi-framework effort into under five months. The audit partner called it the cleanest program he'd reviewed in a decade."

Soren Lindqvist

VP Engineering, Enterprise SaaS

Full reference contact information available upon request. All recommendations verified on LinkedIn: linkedin.com/in/savannamyer