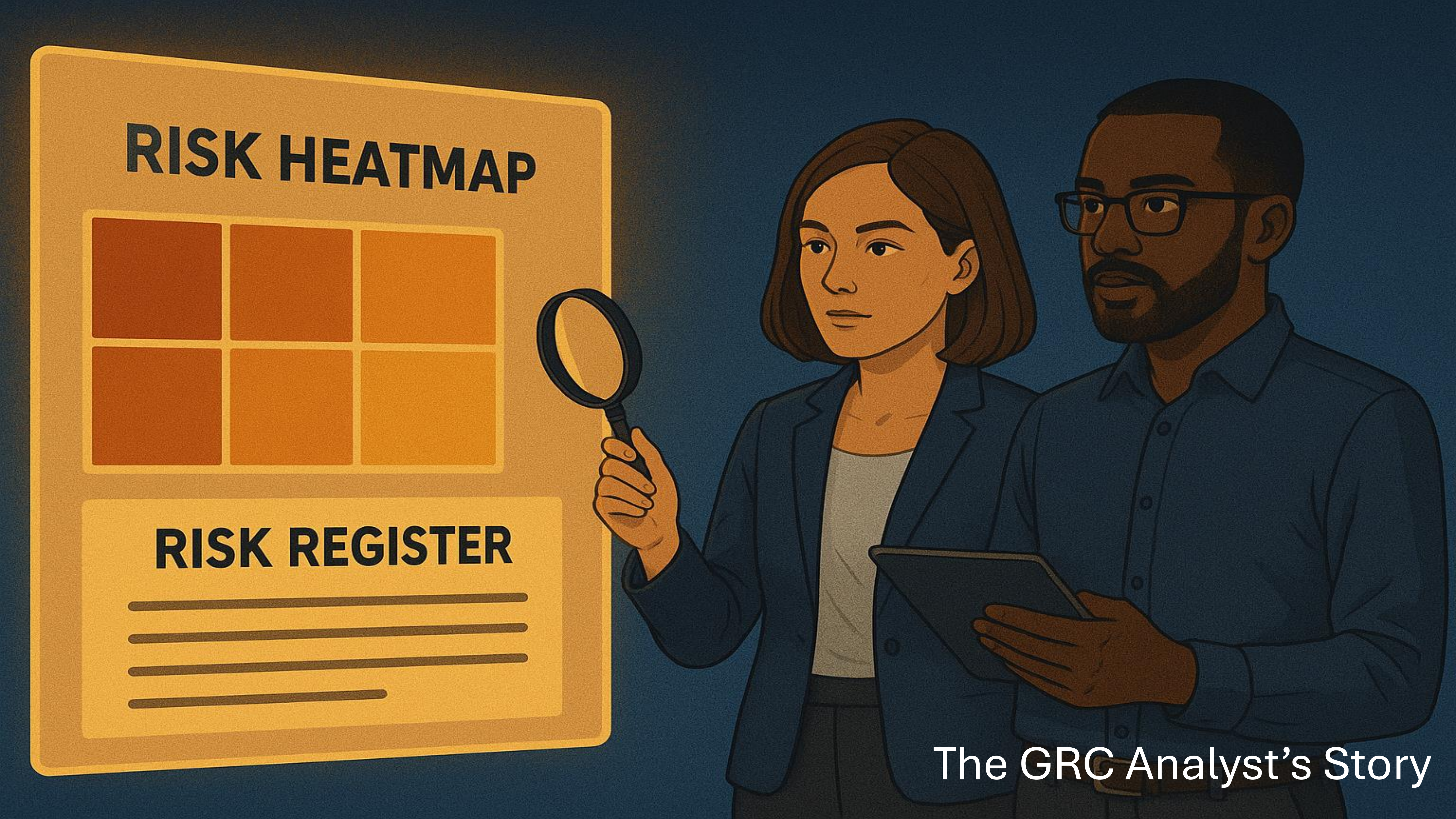
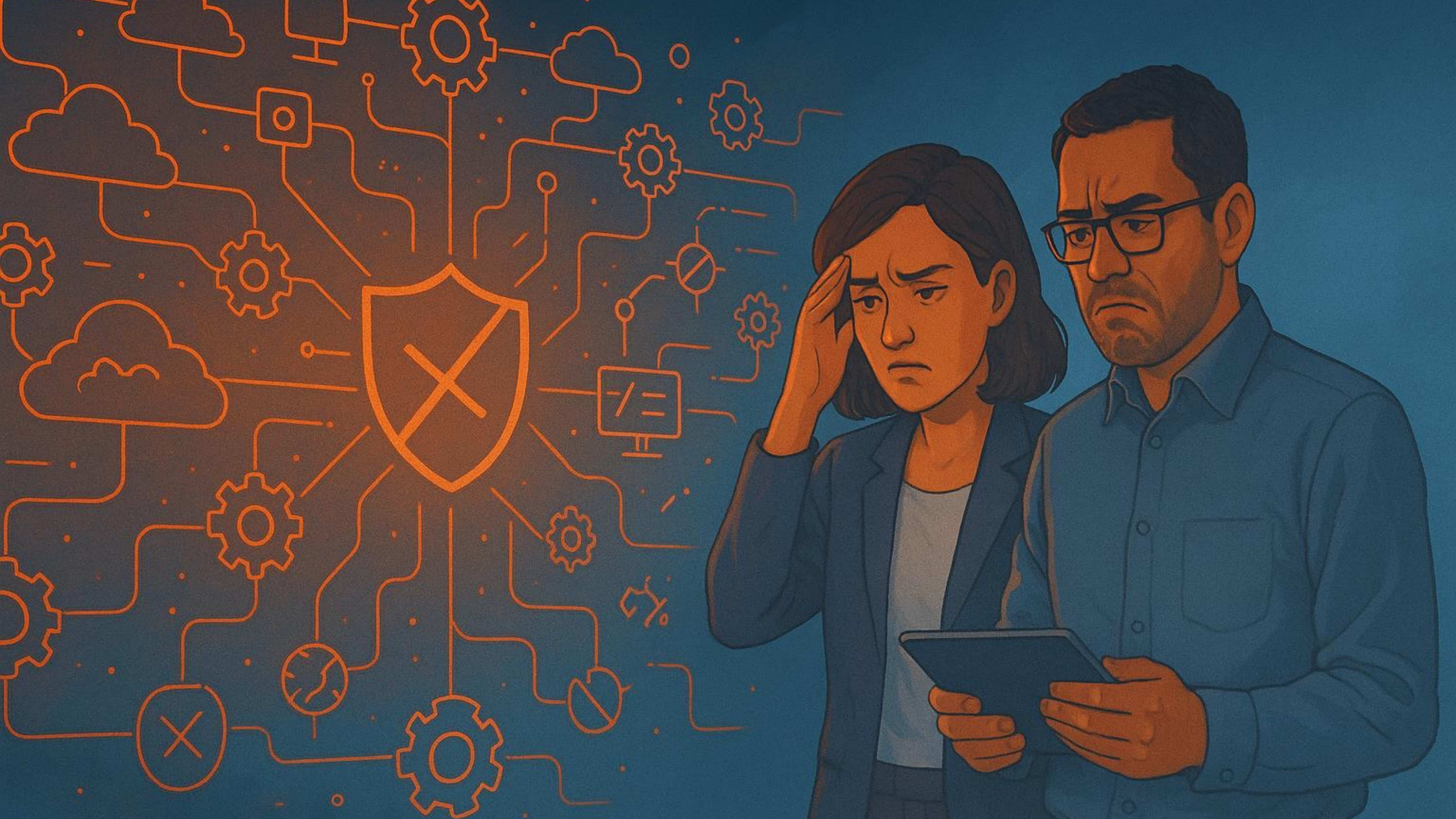
The Unexpected Union: When GRC and Architects Come Together



The GRC Analyst’s Story

RISK REGISTER
Rick
RISK HEATMAP
High
High
Low
Medium
Critical

The Architect’s Story



Some of GRC’s challenges

- Tick-Box mentality
- Reactive involvement
- Technical blind spots

Some of Architecture’s challenges

- Lack of risk context
- Siloed thinking around systems
- Unaware of governance perspectives

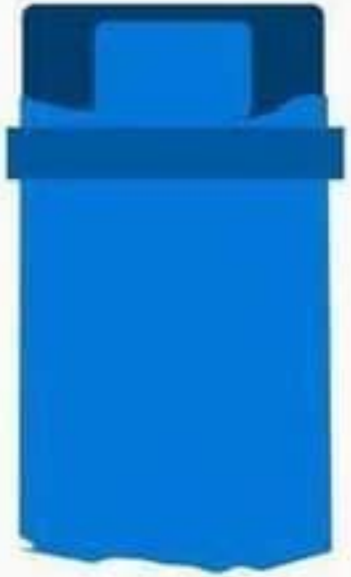
Sleeping Positions

CEO

CFO

COO

CISO



Governance, Risk and Architecture

Certification and Accreditation

Certification and Accreditation (C&A)

Governance, Risk and Architecture (GRA)

- What are the skills that the members of the team brings?
- What problems does this team solve for the organization?
- What is the shared vision and mission for the team?

Persona	Typical Cybersecurity Roles / Functions	Core Strengths in a Security Context	Potential Blind Spots / Risks
Idealist	- **Governance, Risk & Compliance (GRC)** - **Security Awareness / Culture**	- Strong belief in *principles, ethics, and frameworks* (e.g., ISO 27001, NIST CSF) - Advocates “security by design” and trust-based culture - Inspires others toward long-term maturity goals	- Can become frustrated by operational limitations or “checkbox” compliance - May underestimate practical constraints or stakeholder fatigue
Realist	- **Security Operations (SOC)** - **Incident Response / Threat Intel**	- Grounded in *current threats, data, and evidence* - Keeps the organization alert to real-world attacks - Focuses on what’s actually exploitable	- May appear cynical toward strategic or idealistic initiatives - Can deprioritize longer-term culture or design improvements
Pragmatist	- **Security Engineering** - **Security Architecture** - **DevSecOps / Automation**	- Bridges vision with *implementable controls* - Chooses “good enough” solutions that deliver outcomes - Excellent at balancing usability vs. security	- Might over-optimize for convenience, creating technical debt or partial coverage
Skeptic	- **Red Team / Penetration Testing** - **Security Review / Audit**	- Challenges assumptions, “proves it or breaks it” - Exposes design flaws others miss - Vital for defence validation and threat modelling	- Can be perceived as overly critical - Risk of eroding trust if feedback isn’t constructively delivered
Optimist	- **Security Awareness / Communications** - **Leadership / Transformation Roles**	- Motivates teams under pressure - Sees opportunities in crises (“teachable moments”) - Promotes a growth mindset and resilience	- Can underestimate risk or dismiss systemic constraints
Pessimist	- **Risk Assessment / Compliance Assurance** - **Policy & Audit**	- Cautious, detailed, strong scenario analysis - Identifies what could go wrong early - Ensures robust fallback and contingency plans	- May slow innovation or resist automation - Tendency toward “no by default” culture
Humanist	- **Security Leadership / Awareness / HR Liaison** - **Insider Threat / Behavioural Risk**	- Focuses on the *human element* in cyber risk - Designs empathetic awareness and intervention programs - Fosters collaboration between technical and business teams	- Might avoid confrontation or underestimate adversarial behaviour
Objectivist	- **Data Protection / Forensics / Analytics** - **Security Metrics & Measurement**	- Bases security on *data, not opinion* - Excellent at threat hunting, incident forensics, and reporting accuracy - Good alignment with governance metrics and KPIs	- Can appear emotionally detached or overly quantitative - May miss cultural or human nuances behind incidents

Persona	Typical Cybersecurity Roles / Functions	Core Strengths in a Security Context	Potential Blind Spots / Risks
Idealist	- **Governance, Risk & Compliance (GRC)** - **Security Awareness / Culture**	- Strong belief in *principles, ethics, and frameworks* (e.g., ISO 27001, NIST CSF) - Advocates “security by design” and trust-based culture - Inspires others toward long-term maturity goals	- Can become frustrated by operational limitations or “checkbox” compliance - May underestimate practical constraints or stakeholder fatigue
Realist	- **Security Operations (SOC)** - **Incident Response / Threat Intel**	- Grounded in *current threats, data, and evidence* - Keeps the organization alert to real-world attacks - Focuses on what’s actually exploitable	- May appear cynical toward strategic or idealistic initiatives - Can deprioritize longer-term culture or design improvements
Pragmatist	- **Security Engineering** - **Security Architecture** - **DevSecOps / Automation**	- Bridges vision with *implementable controls* - Chooses “good enough” solutions that deliver outcomes - Excellent at balancing usability vs. security	- Might over-optimize for convenience, creating technical debt or partial coverage
Skeptic	- **Red Team / Penetration Testing** - **Security Review / Audit**	- Challenges assumptions, “proves it or breaks it” - Exposes design flaws others miss - Vital for defence validation and threat modelling	- Can be perceived as overly critical - Risk of eroding trust if feedback isn’t constructively delivered
Optimist	- **Security Awareness / Communications** - **Leadership / Transformation Roles**	- Motivates teams under pressure - Sees opportunities in crises (“teachable moments”) - Promotes a growth mindset and resilience	- Can underestimate risk or dismiss systemic constraints
Pessimist	- **Risk Assessment / Compliance Assurance** - **Policy & Audit**	- Cautious, detailed, strong scenario analysis - Identifies what could go wrong early - Ensures robust fallback and contingency plans	- May slow innovation or resist automation - Tendency toward “no by default” culture
Humanist	- **Security Leadership / Awareness / HR Liaison** - **Insider Threat / Behavioural Risk**	- Focuses on the *human element* in cyber risk - Designs empathetic awareness and intervention programs - Fosters collaboration between technical and business teams	- Might avoid confrontation or underestimate adversarial behaviour
Objectivist	- **Data Protection / Forensics / Analytics** - **Security Metrics & Measurement**	- Bases security on *data, not opinion* - Excellent at threat hunting, incident forensics, and reporting accuracy - Good alignment with governance metrics and KPIs	- Can appear emotionally detached or overly quantitative - May miss cultural or human nuances behind incidents

The Spark — Early Curiosity

"It always starts with curiosity."

- Asks *why* things are built a certain way, not just *how*.
- Sees patterns, not tasks.
- Traces problems beyond their own role or team.
- Feels compelled to connect the dots between governance, architecture, and reality.

They're not chasing titles — they're chasing understanding.

The Integrator — Seeing the Whole

"They begin to think like systems, not silos."

- Understands how one control impacts many workflows.
- Uses data to balance compliance, usability, and risk.
- Connects metrics to system telemetry.
- Becomes the bridge others rely on to make sense of complexity.

Governance meets architecture. Risk meets design.

The Bridge — Crossing Boundaries

"They start speaking two languages fluently."

- Learns to translate between policy and design.
- Brings GRC context into architectural thinking.
- Builds credibility across silos — risk, architecture, operations.
- Uses frustration as fuel to integrate instead of complain.

They stop saying "that's not my job" and start asking "how do we align this?"

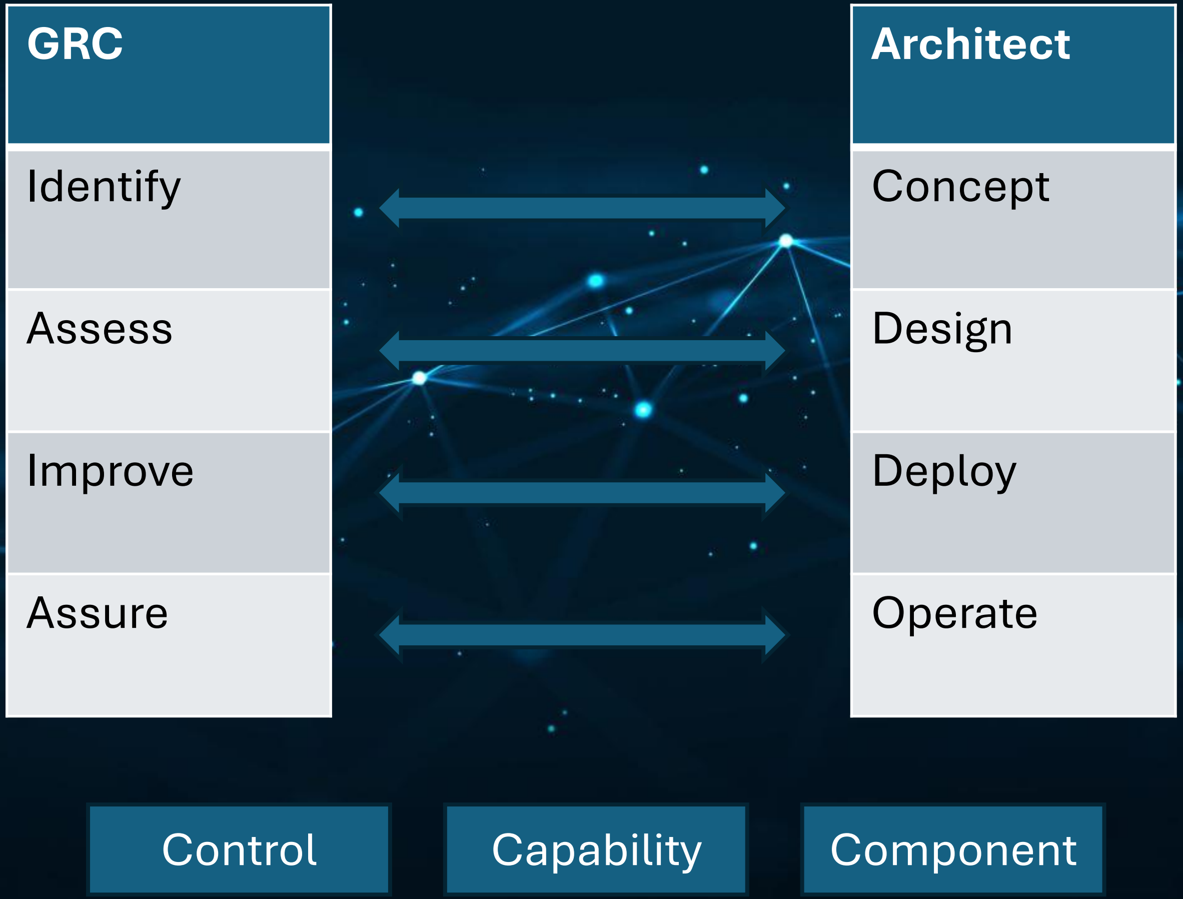
The Unicorn — The Strategic Connector

"They no longer fit in one box — they build the boxes."

- Fluent across domains: technology, governance, risk, leadership.
- Shapes strategy *and* ensures it's executable.
- Mentor others to see connections instead of barriers.
- Operates with empathy, clarity, and systems intelligence.

They embody the fusion of logic, empathy, and vision.

Shared Language and Taxonomy



GRC	Architect
Identify	Concept
Assess	Design
Improve	Deploy
Assure	Operate

Control

Capability

Component

Governance

- Architecture-aligned control catalogue with embedded design rationale.
- Risk-aligned design pattern library (e.g., Zero Trust).
- Decision playbooks for technology adoption and exception handling.

Risk

- Integrated risk assessment linking assets, threats, and architectural mitigations.
- Periodic threat-informed risk dashboards for leadership.
- Cross-domain risk scenarios (e.g., insider threat × cloud misconfiguration).

Architecture

- Based on governance and risk understanding develop maturity roadmap with periodic progress targets.

- Develop security programs that continuously execute defined roadmaps.

- Measures the security program related KPIs and evolve deliverables based on current threats.

Vision

To enable the business where cybersecurity is not a barrier but a catalyst. Empowering innovation, speed, and customer trust through intelligent protection and purposeful design.

An enterprise where governance, risk, and architecture maturity evolve together to form a competitive advantage in its digital offerings.

Mission

To unite strategic governance, intelligent risk management, and purposeful security architecture into a single force that drives transformation.

Turn complexity into clarity, compliance into confidence, and security into a seamless enabler of innovation. Ensuring that trust is not just maintained but engineered into everything we build.

AI
REFERENCE ARCHITECTURE
RISK

Thank You.

Zuoxin (Shawn) Wang

Head of Cybersecurity Governance, Risk and Architecture at Spark New Zealand