Where Governance and Risk Management Align for Impact

Beyond Automation: Real-World Security Gains from AI in GRC

George Totev, CISO
Trustero

Agenda

- The current state of GRC
- Common use cases
- How to select and use AI

(No models were harmed during the making of this presentation)

The Challenge for GRC Teams

Why Our Current Risk and Compliance Approach is Failing

- **Regulatory Proliferation**
  - New regulations pile on faster than teams can adapt
  - Security teams now answer to multiple frameworks, jurisdictions, and auditors - each with their own evidence and control requirements
- **Increased Business Complexity**
  - Large, multinational enterprises, with multiple product lines, in diverse markets
  - Supply chain complexity is growing
- **Technology Complexity**
  - The cloud era has proliferated complex technology stacks
  - AI adoption exacerbates the complexity
- **Scalability**
  - We cannot scale linearly with the organization
  - Other teams are scaling faster

Shadow Risk Acceptance

GRC Teams Should Help Manage, Not Create Risk

- **Risk Management**
  - Do we manage risk or we manage compliance?
  - Explicit vs. Implicit Risk Acceptance
  - Unknown unknowns
- **Organizational Risk**
  - Overburdened SMEs
  - Dissatisfied Partners
  - Unmet expectations - Who knows everything about everything?

Do you manage risk or compliance? Do you generate risk?

Episode III

AI GRC

We Need a Quantitative and Qualitative Jump!

A REVOLUTION in How GRC Teams Operate

Practical Examples

1. How to become compliant? Performing a gap assessment
2. How to stay complaint? Continuous Control Monitoring

Compare efficiency and effectiveness of Traditional, Generic AI, and Expert AI approaches

Gap Assessment

GRC 2025 Conference

Use Case: CCF with SOC2, ISO27001 and PCI. Uplift to NIST 800-53

Approach	Effectiveness	Efficiency	Cost
Consultants (internal/external)	High. The experts will analyze your specific environment and bring relative experience	Low. Usually, it will take a few months and larger team	High. >$100,000
Generic AI	Low. Good at answering high level questions; lacks context. Incomplete	Medium. Prompting and hallucination are challenges.	Low. Unless you want to improve the contextualization.
Expert AI	High. Combines the expertise and contextualization.	High. Could take only a few hours.	Low. AI usage and the expert time.

ISACA | IIA

Continuous Monitoring (ConMon)

GRC 2025 Conference

Use Case: Continuously monitoring controls performance (DE/OE)

Approach	Effectiveness	Efficiency	Cost
Traditional	High. The team will have to match evidence to controls and continuously verify it	Low. While there are evidence workflow tools this is very labor intensive	High. A dedicated team of experts (both SME and environment)
Generic AI	N/A due to sensitivity of contextual data and integrations complexity	N/A	N/A
Expert AI	High. Combines the expertise and contextualization.	High. Could be done by request or continuously.	Low. AI usage only. Experts necessary only if there are anomalies

But wait! There is more…

GRC Benefits

- Inbound/Outbound questionnaire Automation
- Audit Readiness and evidence gathering
- Knowledge retention

Outside of GRC Benefits

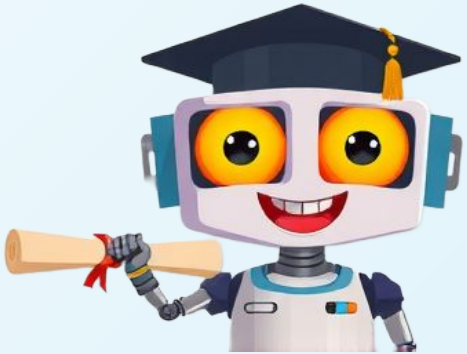
- Security: Tabletop exercise
- DevOps: New product feature
- Legal: Contract Review
- IA: Operational Risk Assessment
- M&A: Acquisition Integration

Context + Prompt + Restrictions + Reasoning

Using AI

1. AI is not a tool; it is a junior member of your team
2. AI will not fix a “broken” GRC program
3. You need a trusted expert
   a. Contextualization
   b. Prompting
   c. Restrictions
   d. Reasoning
4. Workflow, consulting and management
5. Talent and knowledge retention
6. Agents

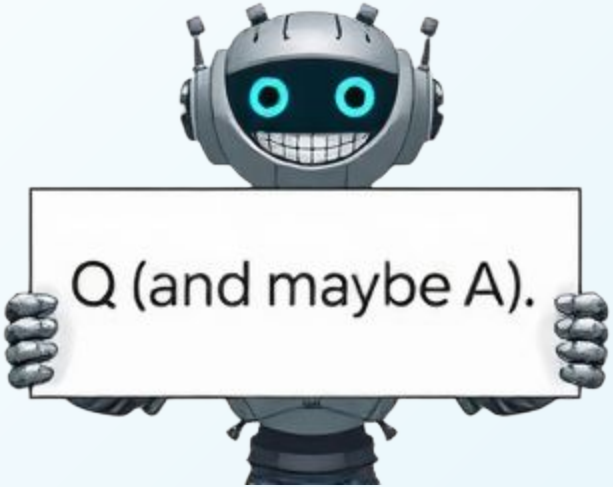
I have “a guy”! But I am still in control



How to evaluate an AI GRC?

1. “The Quad”
   a. Contextualization - internal and external, data integrity and completeness
   b. Prompting - accuracy, ambiguity, brevity
   c. Restrictions - access and delivery, AI security
   d. Reasoning - references, logic flow
2. Flexibility
   a. Ease of deployment
   b. Solving classes of problems
   c. Ability to train
3. “Team fit”
4. Traditional - cost, security, integrations, access, etc.

How would you evaluate a new junior hire?


Q (and maybe A).