

Automating GRC Frameworks: Mapping Cyber Maturity with Human-Centric Platform

Evolving from Fragmentation to Future-Readiness

Presenter: Jatinder Oberoi, a longtime Security Consultant/CISO

Event: CISO Conference - July 2025

Limitations of Traditional GRC

- Rapid Growth = Increased Regulatory Pressure
- Fragmented Tools = Poor Visibility
- Manual Audits = High Overhead
- Third-party Integrations = Elevated Risk

Why Automate GRC?

- Continuous Monitoring & Alerts
- Streamlined Compliance and Audits
- Actionable Dashboards for Leadership
- Improved Cross-functional Collaboration
- Reduced Overhead and Duplication



Human-Centric Risk in GRC

- Behavioural Risks like Phishing and Data Mishandling
- Human Threat Mapping (e.g., Incydr, CultureAI, KnowBe4)
- Adaptive Security Awareness Training
- GRC Maturity Models

Maturity Mapping

- Measure across dimensions, not just controls
- Tailored interventions by maturity level
- Align security investments with business strategy

MATURITY LEVEL 2



Case Study: A Global SaaS Organisation

- Global brand, fragmented compliance processes
- Siloed Systems, Manual Control testing
- Challenges with Vendor Risk Visibility

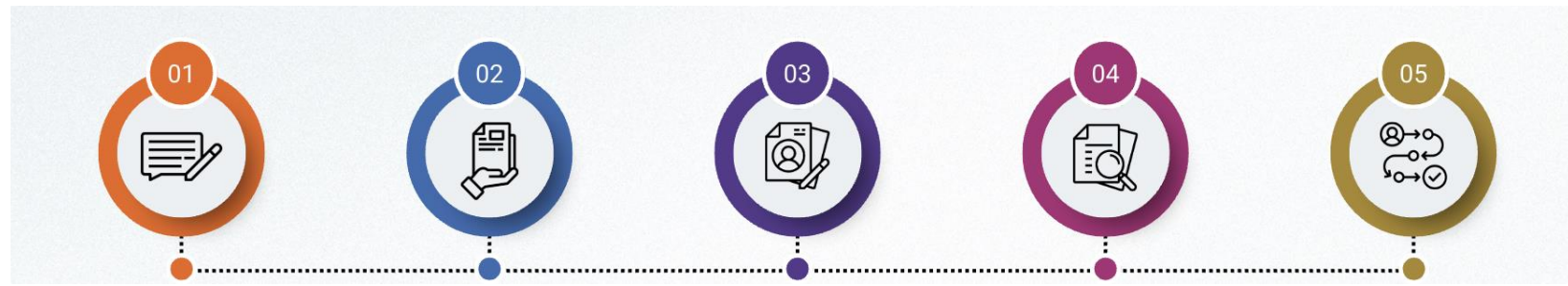
SAAS ORGANISATION

Global Offices



Before Automation

- Risk Register in spreadsheets
- Ad hoc Vendor Reviews
- 6-week SOC 2 Prep Cycle
- Average 3 Escalated Incidents/Year



Transformation Outcomes



- Centralised GRC hub (Jira + Confluence)
- Automated Vendor Risk Scoring
- Quarterly Maturity Reviews
- Role-based Security Training

Transformation Outcomes (Cont'd)

- Unified platform
- Real-time dashboards
- Executive Insights
- Reduced audit fatigue
- Increased readiness

Metric	Before	After
Vendor Reviews	Manual	100% scored quarterly
SOC 2 Prep	6 weeks	2 weeks
Escalated Incidents	3/year	0 in 12 months
Training Completion	65%	98% in 30 days

Results & Metrics

Critical Insights

- Start with what you have
- Maturity across People, Process, Tech
- Embed Security into Product Lifecycle
- Review Periodically

Key Takeaways

- Traditional GRC is no longer sustainable
- Automation unlocks scalability and accuracy
- Human behaviour must be embedded in cyber maturity efforts

Next Steps & Q&A

- . Audit your current GRC posture & Gaps
- . Identify high-friction areas
- . Pilot Automation in one high-risk area
- . Build a Cross-functional GRC culture
- . Explore platforms that support behaviour-based maturity mapping

Connect with
me



[linkedin.com/in/jsoberoi](https://www.linkedin.com/in/jsoberoi)