Pragmatic GRC™ | F-009

The Twelve Principles of Pragmatic GRC™

Every idea in this book traces back to one of the twelve principles below.

1. Business First, Compliance Second (Introduction, Ch. 1, 2, 4)

GRC exists to enable better business decisions, not to create paperwork.

2. Right-Size Everything (Ch. 1, 3, 4)

Every governance activity should match the size, complexity, and risk of the organization.

3. Simplicity Beats Bureaucracy (Ch. 1, 3, 4)

If your GRC program requires a specialist to understand it, it is too complicated for most SMBs.

4. Living Documents, Not Static Documents (Ch. 4, 7)

Documentation should evolve with the business.

5. Governance Is a Daily Habit (Ch. 4, 6)

Governance happens through consistent operational routines, not annual audits.

6. Visibility Before Security (Ch. 2, 4)

You cannot protect assets you don't know exist.

7. Risk Drives Priorities (Ch. 1, 4)

Not every problem deserves equal attention.

8. Accountability Must Be Clear (Ch. 4, 5)

Every asset, risk, and control should have an owner.

9. Measure What Matters (Ch. 6)

Use a small set of meaningful KPIs rather than complex maturity models.

10. Continual Improvement Is Non-Negotiable (Ch. 7)

Governance must evolve as the organization evolves to prevent architecture drift.

11. AI Should Reduce Administrative Burden (Ch. 8)

Use AI to accelerate documentation and analysis while maintaining human accountability.

12. Governance Enables Velocity (Ch. 2)

Good governance removes friction by making decisions repeatable and predictable.