THE PRAGMATIC GRC METHODOLOGY™

The Twelve Principles

A quick reference for why the methodology works the way it does.

1. **Business First, Compliance Second**
   GRC exists to enable better business decisions, not to create paperwork.
2. **Right-Size Everything**
   Every governance activity should match the size, complexity, and risk of the organization.
3. **Simplicity Beats Bureaucracy**
   If it requires a specialist to understand, it’s too complicated for most SMBs.
4. **Living Documents, Not Static Documents**
   Documentation should evolve with the business.
5. **Governance Is a Daily Habit**
   Governance happens through consistent routines, not annual audits.
6. **Visibility Before Security**
   You cannot protect assets you don’t know exist.
7. **Risk Drives Priorities**
   Not every problem deserves equal attention.
8. **Accountability Must Be Clear**
   Every asset, risk, and control should have an owner.
9. **Measure What Matters**
   Use a small set of meaningful KPIs rather than complex maturity models.
10. **Continual Improvement Is Non-Negotiable**
    Governance must evolve as the organization evolves.
11. **AI Should Reduce Administrative Burden**
    Use AI to accelerate documentation while maintaining human accountability.
12. **Governance Enables Velocity**
    Good governance removes friction by making decisions repeatable and predictable.