CyberClean™ Delivery Module

From Regulatory Pressure → Sustainable Cyber Capability

A disciplined, evidence-driven model for closing cybersecurity regulatory findings while building sustainable, regulator-credible capabilities.

MODULE 1 — REGULATORY TRIGGER

Purpose: Establish regulatory reality and scope.

Sources:
- OCC / FDIC / Federal Reserve findings
- MRAs / MRIAs
- Internal & External Audit Issues
- Cybersecurity Incidents
- Consent Orders or Enforcement Actions

Board Perspective:
We begin with regulatory facts — not assumptions or narratives.

MODULE 2 — DIAGNOSE

Purpose: Identify true root causes before action.

Key Activities:
- Root cause analysis
- Cyber risk and control gap mapping
- Control operating effectiveness review
- Evidence integrity assessment
- Risk-based prioritization

Outputs:
- Issue-to-risk mapping
- Validated control failure points
- Regulatory closure roadmap

Board Perspective:
We fix causes, not symptoms.

MODULE 3 — DESIGN

Purpose: Build controls that work in real-world operations.

Key Activities:
- Control redesign or uplift

• Preventive vs. detective control balancing
• Control ownership clarity (1LOD / 2LOD)
• Testing and evidence standards definition
• GRC traceability alignment

Outputs:
• Control blueprints
• Evidence requirements
• Key Control and Risk Indicators (KCI/KRI)

Board Perspective:
Controls are designed to operate, not just exist.

MODULE 4 — DELIVER

Purpose: Execute remediation with accountability and visibility.

Key Activities:
• Agile, sprint-based cyber remediation
• Risk-aligned backlog prioritization
• Evidence production every sprint
• Continuous risk, audit, and compliance engagement
• Regulator-ready documentation

Outputs:
• Implemented cybersecurity controls
• Verified evidence artifacts
• Issue closure packages

Board Perspective:
Progress is measurable, visible, and defensible.

MODULE 5 — SUSTAIN

Purpose: Prevent repeat findings and ensure durability.

Key Activities:
• Control ownership transition to BAU teams
• Automated evidence collection
• Ongoing KCI/KRI monitoring
• Standard operating procedures
• Repeat-finding prevention checks

Outputs:
• Sustainable cybersecurity capability
• Continuous regulatory readiness
• Reduced regulatory friction

Board Perspective:
The program remains effective after transition.

Cross-Cutting Governance & Traceability

Governance and traceability are embedded across all modules:

- Board and Executive Oversight
- Clear accountability across Three Lines of Defense
- Requirement → Risk → Control → Evidence → Metric → Audit traceability