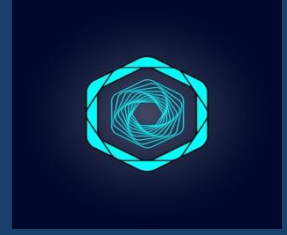
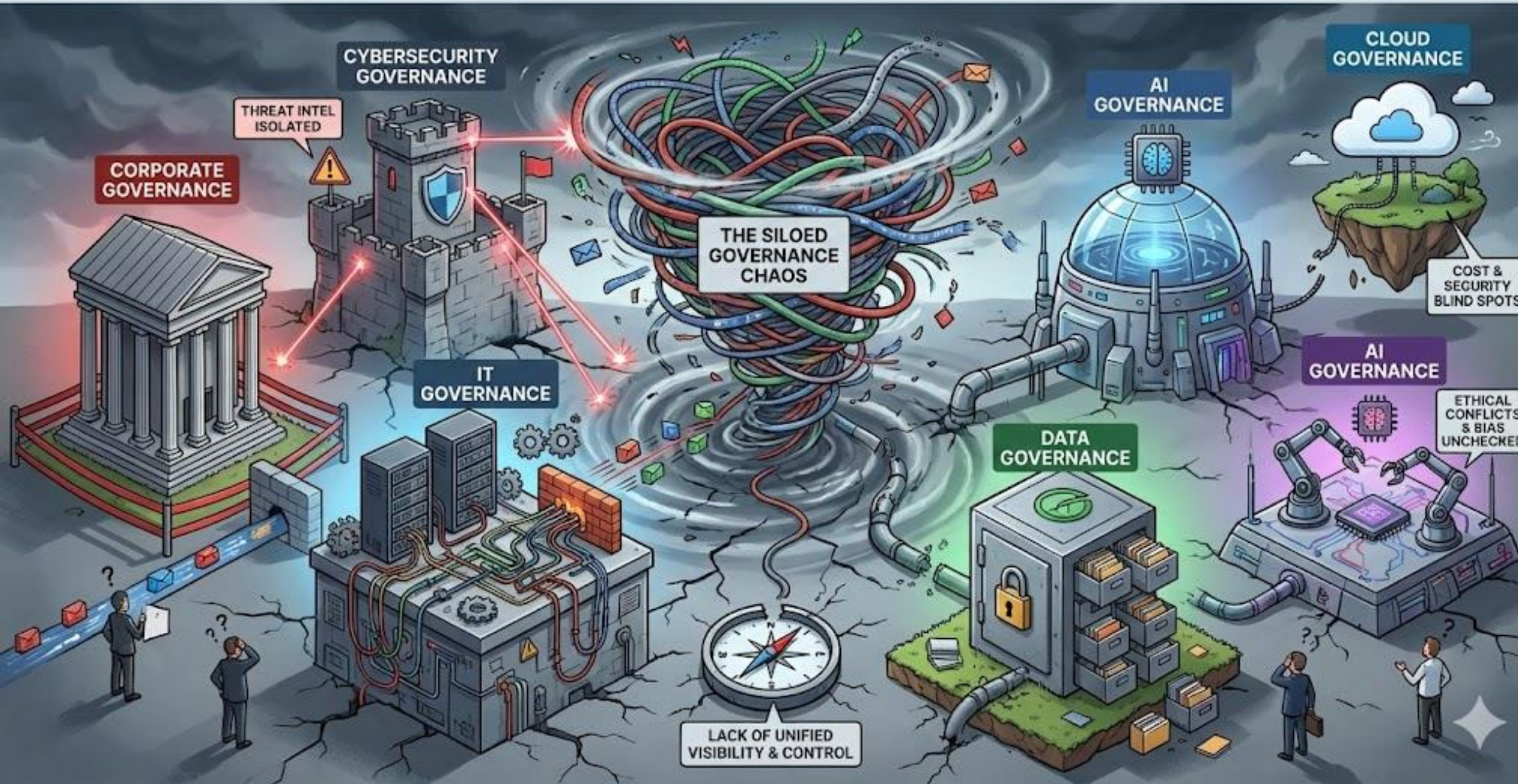
GRC 2.0 and Beyond:
The Shift to Modern Governance, Risk, and Compliance

Aladdin Dandis
Secure Dimension for Management and Digital Consulting



Problem 1: Silos

The Chaos of Siloed Governance: A Multitude of Disconnected Models



The Reality Today: GRC Chaos and Fragmentation

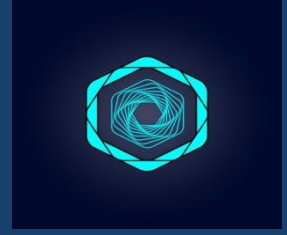
- We are operating in a state of fragmented governance. Multiple departments are managing risk and compliance, but they are doing so in isolation, using different languages, tools, and metrics.

- **The Siloed Landscape:**
  - **IT & Cybersecurity:** Focused on technical controls, vulnerabilities, and threat frameworks (e.g., NIST, ISO 27001).
  - **Regulatory & Corporate Compliance:** Focused on policy adherence, legal mandates, and regulator reporting (e.g., CBJ, GDPR).
  - **Operational Risk:** Focused on business processes, resilience, and manual control testing.
  - **Data Privacy & Governance:** Focused on data flows, consent management, and AI ethics.

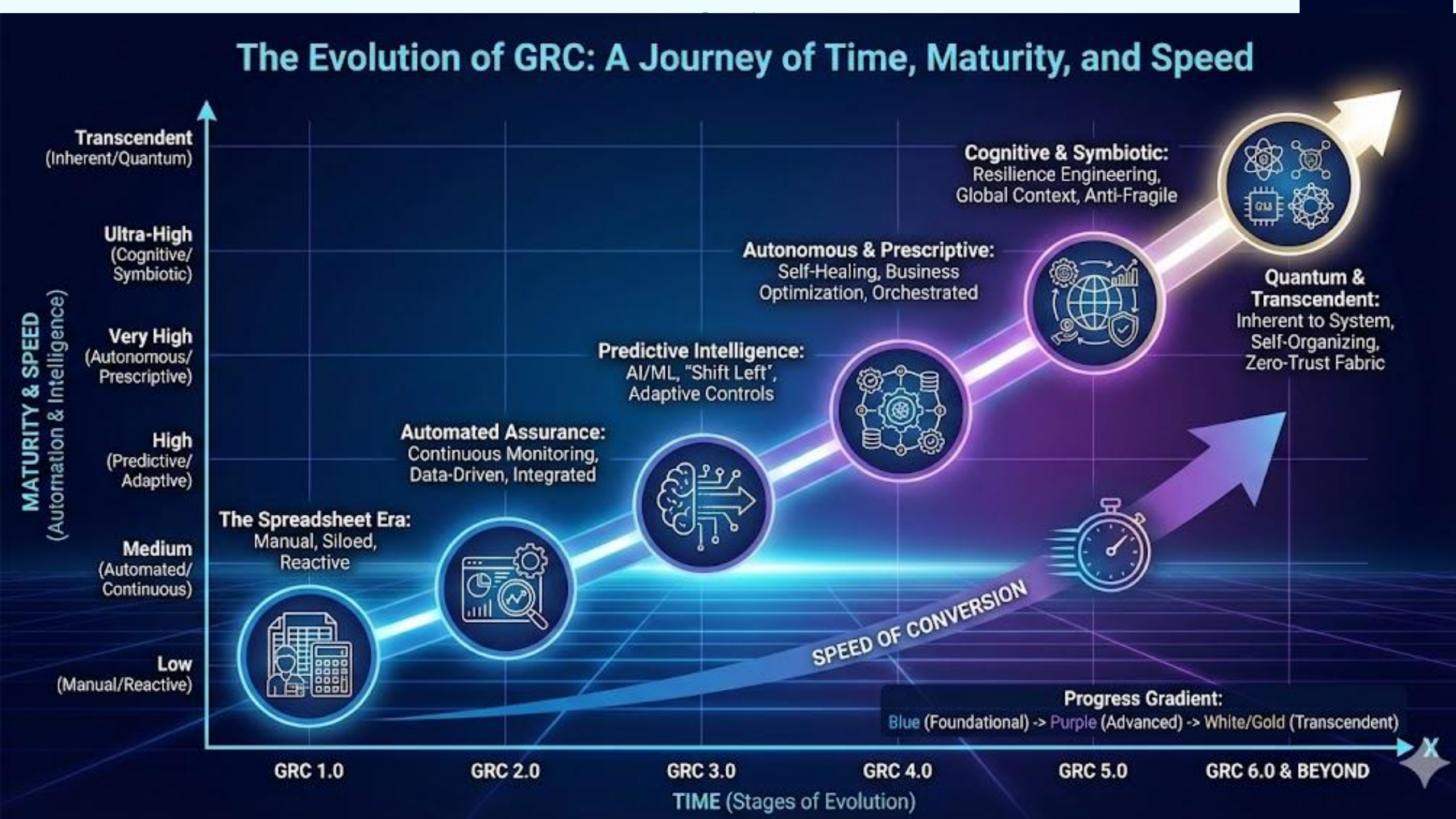
- **The Result:** A fractured view of enterprise risk where critical connections between technical failures and business impacts are missed.

The Business Impact of the Chaos

- Maintaining multiple, disconnected GRC models is not just inefficient; it actively creates risk.
    - **1. Extreme Inefficiency & Audit Fatigue:**
        - Control owners are asked for the same evidence (e.g., "User Access Review") five different times by five different audit teams.
        - Valuable resources are wasted on manual data aggregation instead of risk analysis.
    - **2. The Visibility Gap (Executive Blindness):**
        - Leadership receives fragmented reports. IT says "Secure," Compliance says "Compliant," yet the business is still exposed to systemic risks that fall between the silos.
        - No single "pane of glass" to understand the cumulative impact of risks.
    - **3. Dangerous Latency:**
        - When a new regulation emerges or a cyber threat hits, manually correlating data across silos takes weeks. In a digital world, we need answers in minutes.
- **The Bottom Line:** We are "compliance-rich" in our silos, but "security-poor" across the enterprise.



Problem 2: Transformation


The Evolution of GRC: A Journey of Time, Maturity, and Speed
MATURITY & SPEED
(Automation & Intelligence)
Transcendent
(Inherent/Quantum)
Ultra-High
(Cognitive/
Symbiotic)
Very High
(Autonomous/
Prescriptive)
High
(Predictive/
Adaptive)
Medium
(Automated/
Continuous)
Low
(Manual/Reactive)
The Spreadsheet Era:
Manual, Siloed,
Reactive
Automated Assurance:
Continuous Monitoring,
Data-Driven, Integrated
Predictive Intelligence:
AI/ML, "Shift Left",
Adaptive Controls
Autonomous & Prescriptive:
Self-Healing, Business
Optimization, Orchestrated
Cognitive & Symbiotic:
Resilience Engineering,
Global Context, Anti-Fragile
Quantum &
Transcendent:
Inherent to System,
Self-Organizing,
Zero-Trust Fabric
SPEED OF CONVERSION
Progress Gradient:
Blue (Foundational) -> Purple (Advanced) -> White/Gold (Transcendent)
GRC 1.0
GRC 2.0
GRC 3.0
GRC 4.0
GRC 5.0
GRC 6.0 & BEYOND
TIME (Stages of Evolution)

Context

- The dual pressure on Financial Institutions:
  - Accelerating Regulation: CBJ is aggressively modernizing frameworks (Cybersecurity, Cloud, Fintech, Open Banking, updated AML/CFT).
  - Digital Transformation: Banks are rapidly adopting cloud and digital channels, creating new risk surfaces faster than manual processes can cover.

GRC 1.0 – The "Analog" Era (Legacy State)

- **Reactive Compliance & The Spreadsheet Silos**

- **Context:**
  - Compliance is treated as a "post-event" audit activity to satisfy CBJ inspectors.
  - Risk data is trapped in disconnected Excel sheets across Credit, Ops Risk, and IT departments.
  - CBJ Pain Point: Preparing quarterly reports requires weeks of manual data aggregation, often resulting in lagging, outdated risk views.

- **Main Characteristic:** "Check-the-box" mentality.

GRC 2.0 – Automated Assurance (Current Best Practice)

- **Digitizing the Checklist & Connecting the Dots**

- **Context:**
  - Adoption of dedicated GRC platforms to map controls directly to CBJ regulations (e.g., mapping IT controls to the CBJ Cybersecurity Framework).
  - Basic integration with security tools (SIEM) for continuous monitoring, replacing periodic manual checks.
  - **CBJ Pain Point Solved:** Faster, more accurate reporting on compliance posture, reducing manual audit fatigue.

- **Main Characteristic:** Data-driven, continuous compliance monitoring.

GRC 3.0 – Predictive & Integrated (Emerging Leaders)

- **Anticipating Risk & "Shift Left" Compliance**

- **Context:**
  - Moving from "Are we compliant today?" to "Will we be compliant tomorrow?" using predictive analytics on transaction data and KRIs.
  - Integrating GRC into the software development lifecycle (DevSecOps) for new fintech apps—ensuring CBJ compliance *before* code hits production ("Shift Left").
  - **CBJ Value Add:** Proactively identifying potential breaches or AML/CFT issues before they become regulatory incidents.

- **Main Characteristic:** AI-assisted prediction and integrated risk management.

GRC 4.0 – Autonomous & Prescriptive (The Near Future)

- **Self-Healing Operations & Optimized Risk Taking**

- **Context:**
  - Systems that don't just alert on a CBJ violation, but fix it. (e.g., A cloud configuration drift is detected against CBJ cloud rules and automatically remediated by the platform).
  - GRC tools providing prescriptive guidance: "Based on current market volatility and CBJ liquidity requirements, we recommend adjusting risk appetite in Sector X."
  - **CBJ Value Add:** Drastic reduction in Mean Time To Remediate (MTTR) for compliance gaps.

- **Main Characteristic:** Automated remediation and business optimization.

GRC 5.0 – Cognitive & Symbiotic (Strategic Horizon)

- **The "Brain" of the Resilient Bank**

- **Context:**
  - GRC systems with cognitive understanding of the broader impact of regional geopolitical events on the bank's liquidity and operational resilience.
  - Moving beyond "robustness" (surviving a shock) to "anti-fragility" (improving because of shocks), aligning with advanced Business Continuity planning expectations.
  - **CBJ Value Add:** A banking sector that is deeply resilient to systemic shocks, requiring less external intervention.

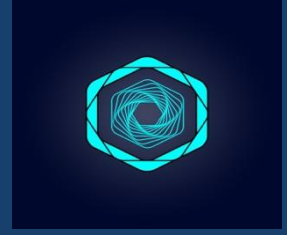
- **Main Characteristic:** Resilience engineering and strategic alignment.

GRC 6.0 & Beyond – Quantum & Transcendent (Future Vision)

- **Inherent Trust in a Decentralized Financial Future**

- **Context:**
  - Preparing governance structures for the post-quantum cryptography era to protect customer data held under local regulations.
  - Governance embedded into the fabric of transactions themselves, perhaps via smart contracts in future CBJ-led digital currency initiatives (CBDC).
  - **CBJ Value Add:** "Compliance by Code"—the system cannot process a non-compliant transaction.

- **Main Characteristic:** Zero-Trust fabric and inherent governance.



Thank You

Aladdin Dandis, Secure Dimension

adandis@secdimension.com