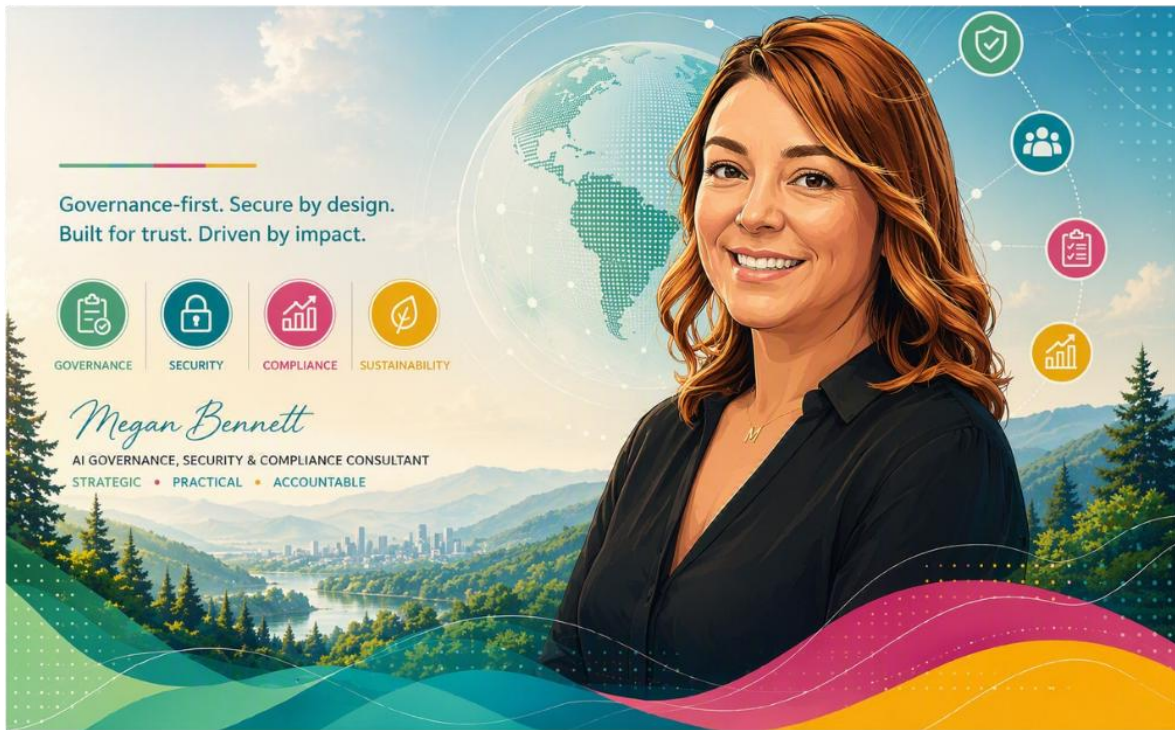




Megan Bennett

253.225.2623

AI Governance, Security & Compliance

My work aligns with Microsoft's AI governance, security, and service-level expectations, including responsible AI use, Zero Trust architecture, and secure operation of cloud and AI services.

This approach treats AI governance as part of operational risk management, ensuring compliance and accountability.

Environmental Compliance & Sustainability

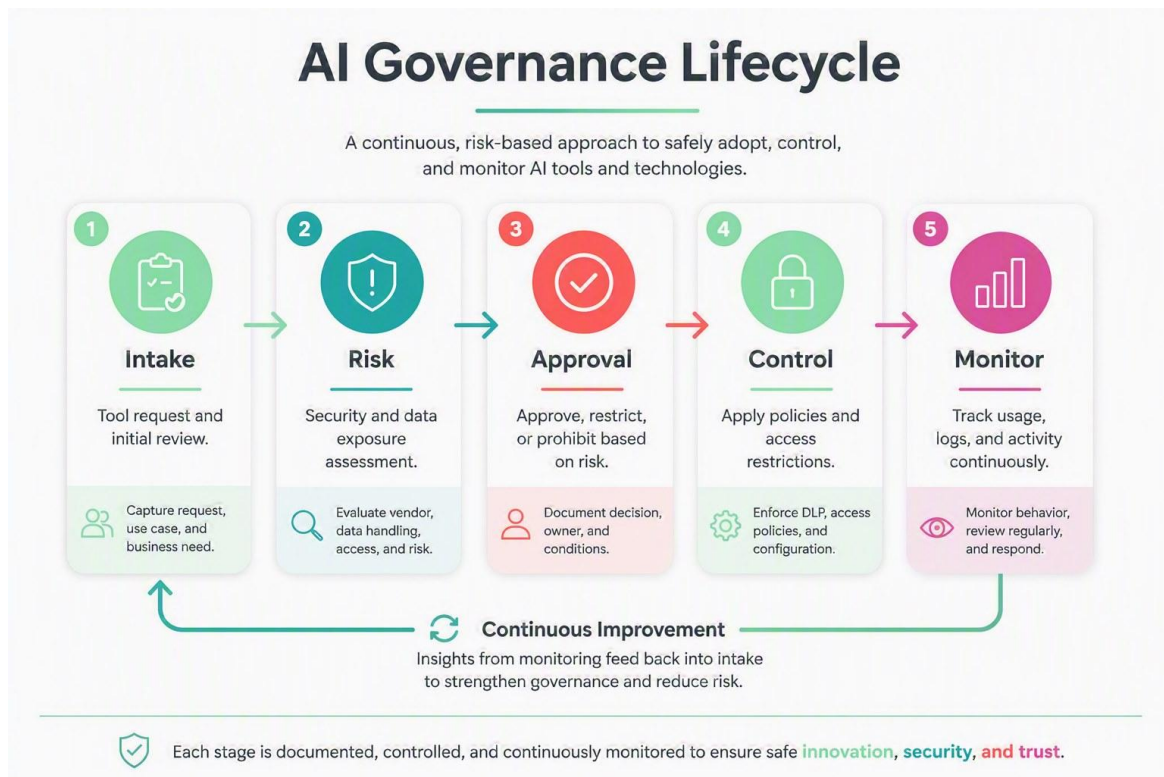
Environmental compliance requirements are addressed in alignment with Microsoft's Service Level Disclosure and Emissions Reduction Plan expectations, including supplier reporting through the Microsoft Supplier Emissions Portal.

This approach treats environmental compliance as part of operational governance, not a standalone checkbox, so it can scale across enterprise and public-sector environments.

What I Do

I support clients in:

- Translating AI risk and regulatory expectations into practical governance controls
- Establishing security and access models for AI-enabled systems using Zero Trust principles
- Aligning AI, data, and cloud use with responsible, compliant operational practices
- Preparing audit-ready documentation that connects AI governance, security, and enterprise compliance
- Translating environmental requirements into practical governance controls.
- Supporting sustainability and emissions reporting tied to technology and vendors.
- Aligning AI, data, and cloud use with responsible environmental practices.
- Preparing audit-ready documentation that connects environmental, data, and security compliance



CORE EXPERTISE

AI Governance & Risk Management

- AI tool intake, review, approval, and lifecycle tracking
- Risk classification, documentation, and registry management
- Alignment with ISO/IEC 42001 and responsible AI principles
- Audit-ready governance and compliance support

Microsoft Security & Compliance

- Microsoft Purview (data protection, DLP, labeling)
- Entra ID (identity, Conditional Access, RBAC)
- Microsoft Defender (threat detection and monitoring)

Zero Trust Security

- Identity-first access and least-privilege enforcement
- Device compliance and access validation
- Continuous monitoring and verification

AI Security in Practice

- AI used as a productivity tool—not a decision-maker
- Data protection controls applied to AI inputs and outputs
- Secure AI agent design and governed usage policies

Environmental Compliance & Sustainability Governance

- Environmental compliance aligned with Microsoft Service Level Disclosures and Supplier Emissions Portal reporting
- Creation and maintenance of Emissions Reduction Plans grounded in operational and vendor realities
- Facility and energy oversight, including baseline controls, usage tracking, and periodic audits
- Practical solutions to meet baseline vendor sustainability expectations without introducing operational risk

- Championing initiatives that deliver measurable emissions reductions
- Clear, plain-language communication with corporations on renewable resources and clean energy tradeoffs
- Translation of environmental requirements into governed, auditable practices that scale across enterprise and public-sector environments



AI GOVERNANCE FRAMEWORK

AI governance is embedded into day-to-day operations, not layered on afterward. My work focuses on clear ownership, documented risk decisions, enforced controls, and audit-ready evidence so AI can be used safely without slowing the business.

- Governed AI intake and approval
- Risk-based classification and documented decisions
- Enforced controls using Microsoft security tooling
- Continuous visibility and audit readiness

SECURITY ARCHITECTURE

Governance-First Security Model

Security is embedded into daily operations, not added after the fact. Controls are intentional, documented, and enforceable.

Identity-Centered Protection

- Identity-first access model using MFA, Conditional Access, and role-based access
- Least-privilege enforcement aligned to business roles and risk

Zero Trust in Practice

- No implicit trust across users, devices, or applications
- Every access request verified and continuously evaluated
- Session and device posture validated before access is granted

Centralized Security Control

Security controls are centrally managed and monitored to ensure consistency, visibility, and audit readiness across environments.

Protected assets include:

- Identities
- Devices
- Applications
- Data

AI + POWER PLATFORM GOVERNANCE

Controlled AI Environment

AI operates within defined and secured boundaries.

Data Protection Controls

- Data Loss Prevention (DLP) policies
- Approved connectors only
- Controlled data pathways

Secure AI Agent Model

- Least privilege access
- Logged and monitored interactions
- Restricted data exposure

Policy-Driven AI Usage

AI agents are:

- Predictable
- Controlled
- Accountable

Key Idea: AI operates inside controlled lanes—not open environments.

ALIGNMENT TO STANDARDS

Industry Alignment

This work aligns with:

- ISO/IEC 42001 (AI Management Systems)
- OECD AI Principles
- Zero Trust frameworks
- Microsoft security best practices

What This Demonstrates

- Traceability → decisions are documented
- Transparency → risks are known
- Reliability → outcomes are controlled
- Accountability → ownership is defined

CLIENT VALUE

What This Means for Clients

- Data is protected and controlled
- AI is used responsibly
- Work remains human-centered
- Systems are audit-ready
- Risk is actively managed

Commitment We don't just use AI, we make it safe, predictable, and aligned with your business.

Ask how I can make AI safe, predictable, and aligned with your business



AI should accelerate work, not replace judgment.

Governance should enable innovation, not block it.

Security should be intentional, not reactive.

What Most Companies Get Wrong

- Tool sprawl
- No governance
- Over trusting AI
- Ignoring data exposure

Ask me how I can help your business meet environmental compliance and steward a responsible path forward



I help organizations meet environmental and supplier compliance requirements with practical, audit-ready solutions—without disrupting how the business operates.

From emissions reduction planning to supplier disclosures and energy baselines, my focus is on clear expectations, measurable outcomes, and defensible reporting.