AuditCon

by ACUA

Louisville Kentucky | September 14-18, 2025

ACUA

Data Integrity

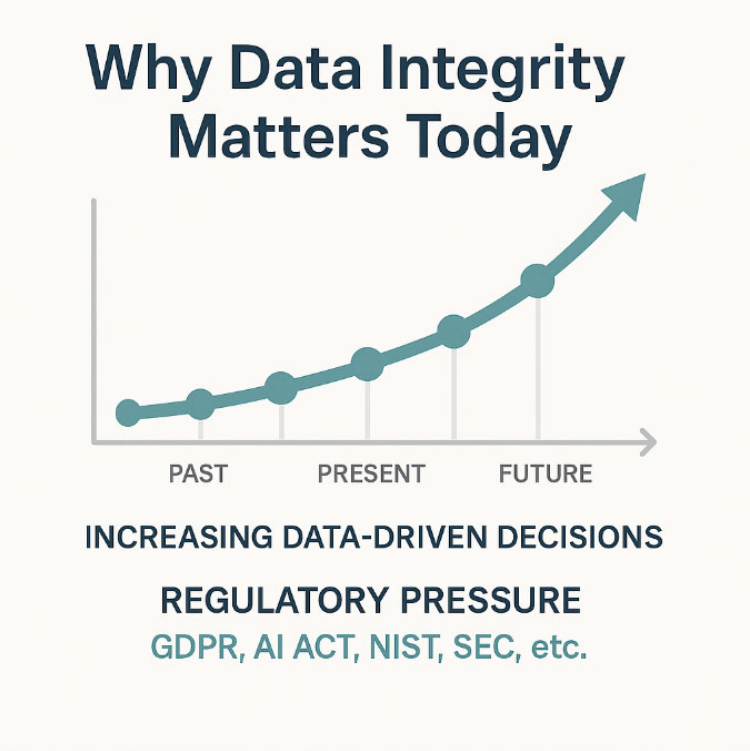
Trusting your Data

PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Presenter:
Mark Bednarz, MS, CPA, CISA, CFE
Partner
mbednarz@pkfod.com

Why Data Integrity & Data Quality?

- HIPAA Internal Audit
- IPEDS Audit
- Procurement Audits
- Privacy Audits



Auditor’s Role in the Digital Age

- Leverage analytics to identify patterns, trends and anomalies in large data sets
- Support risk assessment, project scoping, early detection of potential issues
- Evaluate data integrity across digital systems and emerging technologies
- Anticipate risks associated with automation and AI and advocating and ensuring transparency and trust

Challenges of the Digital Age

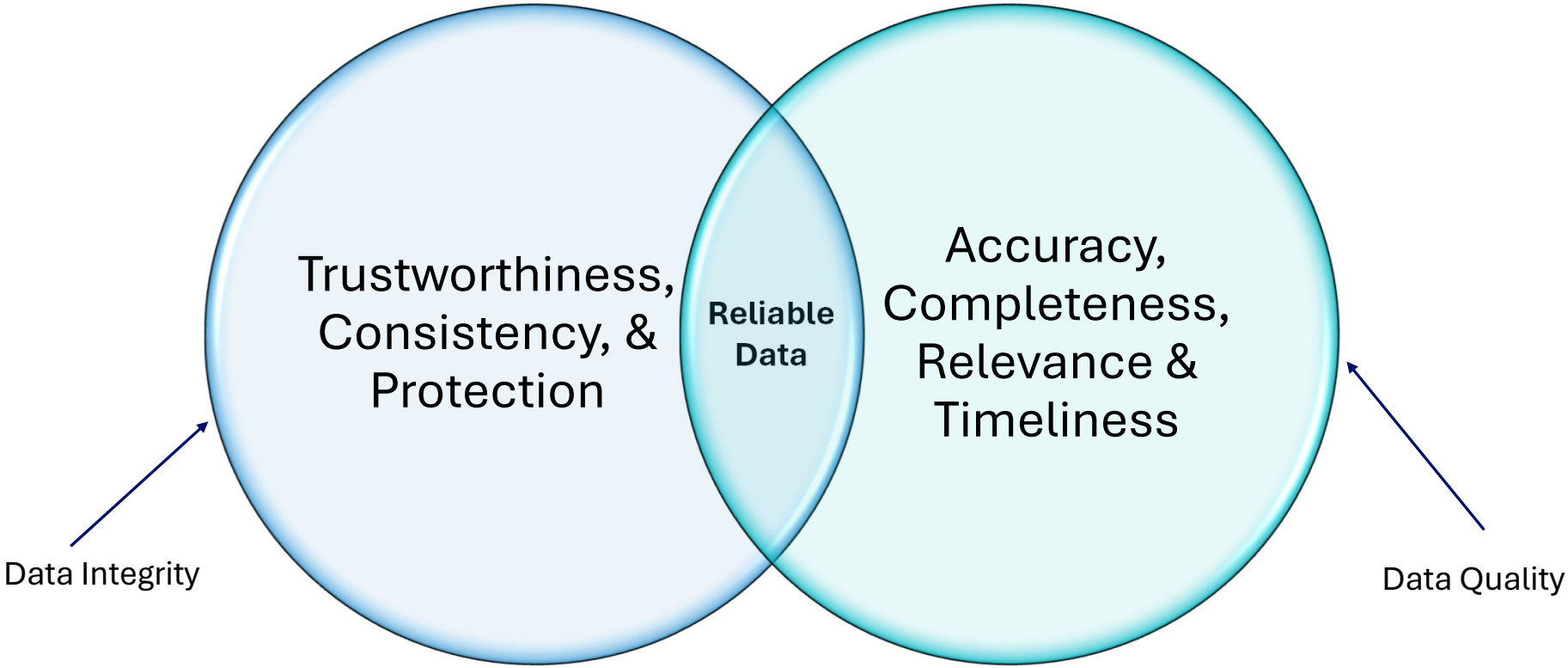
- Data origin and lineage are often unclear
- Reliability and completeness of data may be uncertain
- Multiple versions of data challenge the “single source of truth”
- Difficult to integrate data (i.e., data silos)
- Emerging technologies (AI, automation, cloud) amplify risks when data is flawed
- Talent shortage for collecting, managing, and analyzing data
- Protecting sensitive information and complying with regulations

Data Governance Considerations

Provides a foundation for auditing digital and AI-driven processes

- Establishes policies, standards, and procedures to preserve data integrity
- Defines ownership, stewardship, and accountability for data assets
- Embeds decision rights and responsibilities across the institution
- Process for protecting data from unauthorized access
- Enforces quality checks, validation, and monitoring at all stages of data use

Data Integrity & Data Quality



Data Integrity & Data Quality – Contd.

- **Data Integrity Controls**
  - 🔐 Access restrictions & authentication
  - ✔️ Checksums & validation rules
  - 📜 Audit trails & version controls
  - 🔒 Encryption & backups

- **Data Quality Controls**
  - 🧹 Cleansing & deduplication
  - 📏 Standardization (consistent formats)
  - ✅ Validation rules (completeness & correctness)
  - 🔎 Regular audits & reconciliation

Including Data Integrity & Data Quality Checks In Your Internal Audits

Approach

Roadmap

1. Scope & Planning
2. Governance Policy
3. Data Inventory
4. Access Controls
5. Data Quality Checks
6. Change Management & Audit Trail

Scoping and Planning

- Define audit objectives
- Identify systems, processes, departments
- Align scope with relevant compliance standards/regulations

Data Governance Policy

- Confirm if a formal policy exists
- Data security and privacy
- Evaluate enforcement, access & accountability
- Processes for monitoring, completeness and timeliness

Data Inventory

- Identify all data sources & repositories
- Review data flow diagrams
- Assign clear data owners/stewards
- Structured or unstructured data

Access Controls

- Role-based access defined & enforced
- User access logs reviewed regularly
- MFA implemented for critical systems

Change Management and Audit Trail

- Ensure system change logs are enabled & reviewed
- Verify critical data changes tracked (timestamp + user ID)
- Confirm logs are stored securely and protected

Data Quality Check

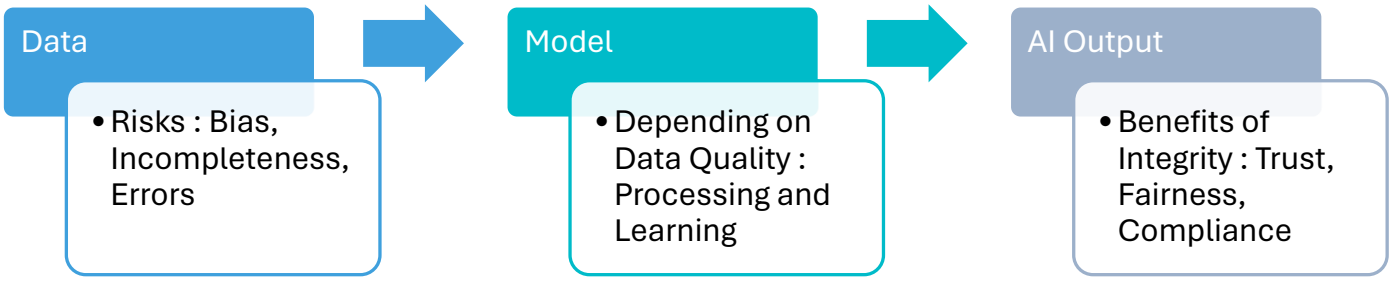
- Validate data against source systems
- Identify duplicates, anomalies, inconsistencies
- Confirm automated validation rules are working

Transition to AI

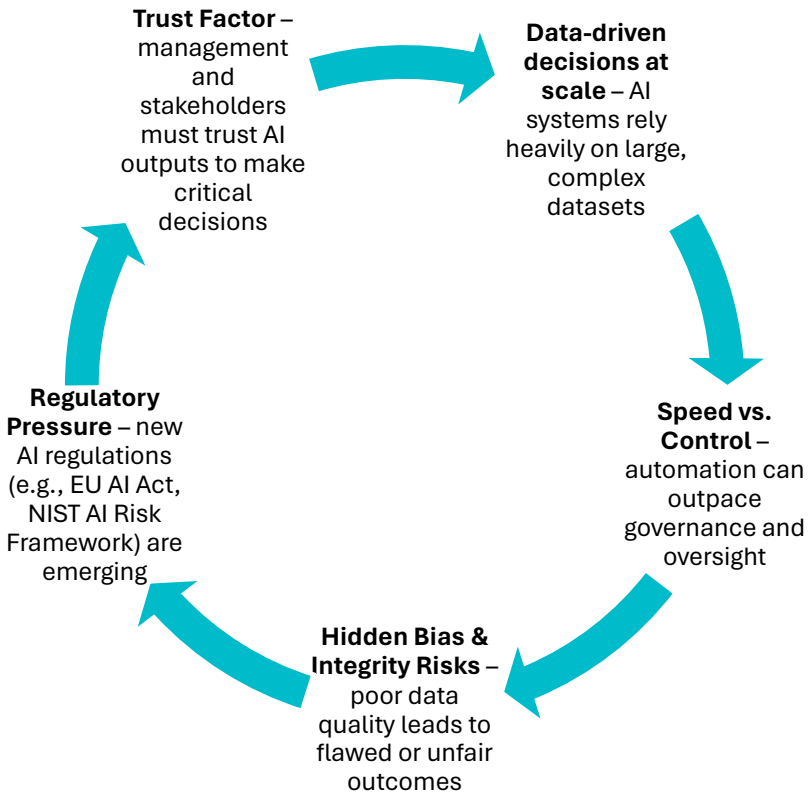
- Strong data integrity & quality controls are the **foundation**
- Without them, AI models inherit flawed data → flawed results
- Auditors must expand scope from traditional data checks → to AI systems

Why Data Quality and Integrity Matter in AI

- **AI depends on data**: “Garbage in, garbage out.” Poor-quality data leads to biased, unreliable AI outcomes.
- **Regulatory & ethical pressure**: Regulators expect transparency in AI-driven decisions.
- **Trust in AI**: High-integrity data underpins explainability, fairness, and compliance.
- **Business impact**: Inaccurate data → flawed AI models → wrong decisions → reputational & financial risk

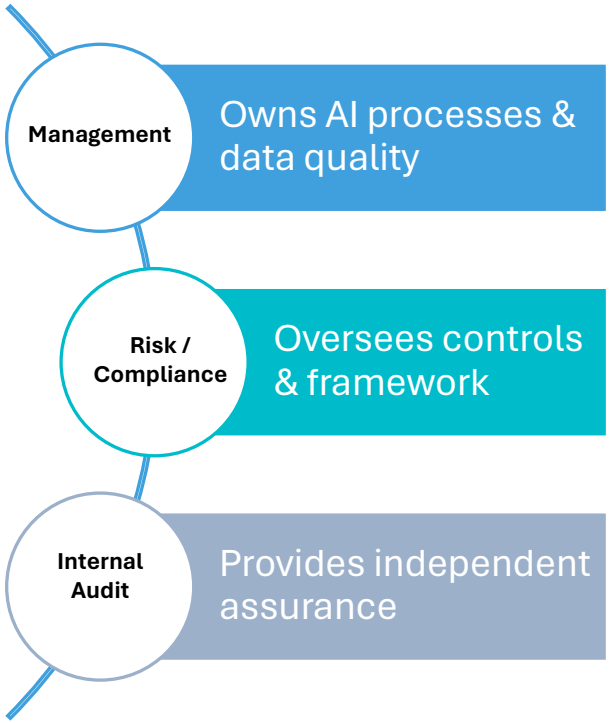


AI Integrity Starts with Data Integrity?



Auditor’s Role in Auditing AI (High-Level)

- **Understand AI systems**
  - What data sources feed the model?
  - How is data prepared, transformed, and validated?
- **Assess Data Integrity Controls**
  - Accuracy, completeness, timeliness, lineage, and governance of AI data.
- **Evaluate AI Governance**
  - Bias testing, validation procedures, and monitoring of outputs.
- **Check Compliance & Accountability**
  - Alignment with frameworks (NIST AI RMF, EU AI Act, SOX, ISO AI).
  - Roles and responsibilities for AI oversight.
- **Report & Recommend**
  - Highlight data risks in AI initiatives.
  - Suggest improvements to controls, governance, documentation, and monitoring.



AI Risk Management

Key Risks

- **Data Quality & Integrity** → Biased, incomplete, or incorrect training data leads to flawed outputs
- **Transparency & Explainability** → "Black Box" models limit auditor oversight
- **Compliance & Ethical Risks** → Regulatory gaps, fairness, discrimination issues
- **Security Risks** → Adversarial attacks, data poisoning, model theft
- **Operational Risks** → Over-reliance on AI without human oversight

Key Takeaways : What You Can Do Tomorrow

As an Auditor, you should:

- **Embed data integrity and data quality checks** into every audit
- **Challenge data lineage** – ask where the data came from and how it was transformed
- **Review data governance roles & responsibilities** (owners, stewards, custodians)
- **Assess data cleansing and preparation processes** for repeatability and documentation
- **Evaluate AI/automation use cases** – test data quality, explainability, and evaluate results

Q & A / Discussion

If you can’t trust the data, you can’t trust the decisions