Data Governance & Compliance
Managing Risk Through Oversight and Control

Alice E. Herring
Enterprise Data Governance Manager
UNCG Information Technology Services

IST 466 Information Ethics & Policy
October 20, 2022
Agenda

Data as an Asset
The What and Why of Data Governance?
Compliance Assurance & Security
Regulations & Policies
UNCG Data Governance Framework
Data Strategy
Access & Security
Introduction: Data as an Asset

• Data is the foundation of knowledge and wisdom for an organization.
• Data is an asset that must be managed and protected.
• Data Governance allows us to manage and ensure the integrity and security of institutional data.
• Data Governance provides us a vehicle to manage risk and compliance.
What is Data Governance?

- A framework to coordinate and oversee the management of data
- An organizational initiative in support of the access and use of data
- A structure for effective and efficient decision making
- A mechanism to manage risk and compliance
- A quality control discipline
Why do we do Data Governance?

- Formalized accountability
- Improved operational efficiency and effectiveness
- Consistent authority over data
- Improved data quality, understanding, and confidence
- Risk management
  - Increased protection
  - Compliance assurance
Compliance Assurance & Security

- State & Federal Regulations
  - FERPA
  - HIPAA
- UNC System Policies
  - 1400.1-3 Information Technology, Security, and Identity & Access
- UNCG Policies & Standards
  - Information Security Policy
  - ISO 2700X Standards
  - Data Classification Policy
- International Regulations
  - GDPR

Image by Gerd Altmann from Pixabay
Federal and International Privacy Regulations

- Family Educational Rights & Privacy Act (FERPA)
- Health Insurance Portability & Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR) - EU
State Statute & UNC System Policies

- N.C. General Statute 116 – Higher Education Act
  - Section 40.22.d – Management Flexibility, Information Technology
- UNC System Policy Manual
  - Chapter 1400.1-3 Information Technology
UNCG Policies & Standards

Policies
- Information Security Policy
- Enterprise Systems Policy
- Acceptable Use of Computing and Electronic Resources Policy

Standards
- Information Security Management Standards
- Access & Authorization Standard
<table>
<thead>
<tr>
<th>UNCG Data Governance Policies, Standards, and Charter</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Governance Structure Policy</strong></td>
</tr>
<tr>
<td><strong>Data Classification Policy</strong></td>
</tr>
<tr>
<td><strong>Data Integrity Policy</strong></td>
</tr>
<tr>
<td><strong>Metadata Collection and Management Standard</strong></td>
</tr>
<tr>
<td><strong>Data Integration Standard</strong></td>
</tr>
<tr>
<td><strong>Data Governance Charter</strong></td>
</tr>
</tbody>
</table>
Executive
Senior most level knowledge of the program

Strategic
Representation from cross-campus units
Enterprise level Data Governance and data management related strategy, policy, standards, processes

Operational
Data definers, producers, users as part of their job responsibilities
Data specific knowledge holders

Data Trustees

Data Stewards

Technology Custodians
Members of ITS and distributed technology specialists across campus
Enterprise technology management
IT Governance

Working Groups
Permanent or time-limited working groups created for specific initiatives

IT Governance

Data Governance Framework

Governance Custodians
Enterprise Data Governance team members

Tactical
Data classification rules, compliance rules

Tactical
Data definitions, business rules, quality rules

You can read more about Seiner’s model online here: https://tdan.com/the-non-invasive-data-governanceo-operating-model/12210
Data Trustees Committee

Responsibilities
- Senior Level officials
- Develop Data Governance Strategy
- Data Governance Policies & Standards
- Promote Resource Management
- Strategic Key Performance Indicators
- Oversee Data Access
- Oversee Data Classification Levels, Storage & Handling

Decision Areas Include
- Review & Support Decisions of Data Stewards
- Establish Policies & Standards
- Align Data Strategy with University Strategic Plan
- KPI Development & Reporting
- Data Access Request Approval
- Data Classification Levels, Storage, & Handling Approvals
Data Strategy

- Timely and accurate information
- Strengthen governance and accountability
- Ensure compliance to regulation and policy
- Support a culture of informed decision making

Image by Gerd Altmann from Pixabay
Improving Data Access & Security

- Confidentiality
  - Prevent unauthorized disclosure
- Integrity
  - Prevent undetectable modification
- Availability
  - Ensure information availability

- L1: Public
  - Such as Public Websites, Published Research, Marketing
- L2: Internal
  - Such as Business Records, Org Charts, Contracts, Budgets
- L3: Confidential
  - Such as FERPA, Employee Reviews, Intellectual Property
- L4: Restricted
  - Such as SSN, PII, PHI, PCI, GLBA, CUI, FISMA
Access & Authorization

- Two-Factor Authorization
- Information Security Management Standard
- Security Classes
- Access Management Software
- Secure Desktop
- Security Awareness Training
Questions?
References

References

• UNCG. (2022, September 12). *Access and Authorization Standard*. UNCG Service Now Knowledge Base. https://uncg.service-now.com/kb?sys_kb_id=5fe3cba01b1e1110470a4267cc4bc0)&id=kb_article_view&sysparm_rank=1&sysparm_tsqueryId=26480bde1b625194989186e9cd4bc05b
Find your way here