



NCYTE CENTER

National Cybersecurity Training & Education Center

BRICCS Research Data
Management Conference (2025)
July 9th – 11th, 2025





Securing the Research Data Lifecycle

Integrating Cybersecurity Standards, Frameworks, and AI into Research Data Management Workflows

Stephen Miller NCyTE Consultant

July 11, 2025



Executive Summary

Research data is a vital asset and prime cyber target.

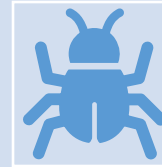
Inadequate security threatens integrity, privacy, and compliance.

Integrating cybersecurity and AI into RDM is crucial for trust and resilience.

Research Data Lifecycle Vulnerabilities



Collection: Sensor spoofing, injection attacks.



Processing/Analysis: Insider threats, malware in scripts.



Storage/Sharing: Misconfigured clouds, unencrypted data.



Archiving/Disposal: Residual data exposure.

Strategic Integration Approaches (Overview)

Strategic Integration Approaches

Approach	Description
Secure-by-Design Planning	Embed cybersecurity in Data Management Plans (DMPs) from inception, including risk assessments based on the CIA triad—confidentiality, integrity, and availability (NIST 2021)
Automated Risk Assessment	Modernize both security and compliance through “rules as code” pilot that recognizes that an opportunity exists to modernize both security and compliance through open, machine-readable formats that streamline control-based risk assessments, such as NIST’s Open Security Controls Assessment Language (OSCAL).
Data Classification and Access Control	Apply sensitivity labels and role-based access, using encryption and multifactor authentication (ISO, 2019)
Safe Collaboration	Use secure protocols (HTTPS, SFTP) and institutional tools for data sharing
Incident Response Preparedness	Define institutional cyber incident response protocols tailored to research
Policy and Standards Alignment	Align with frameworks such as NIST SP 800-171, ISO/IEC 27001, and agency-specific policies (Yang et al., 2019)

Secure-by-Design & Automation

- Integrate cybersecurity into DMPs from inception.
- Use threat modeling and CIA triad.
- Automate risk assessments with 'rules as code' and OSCAL.

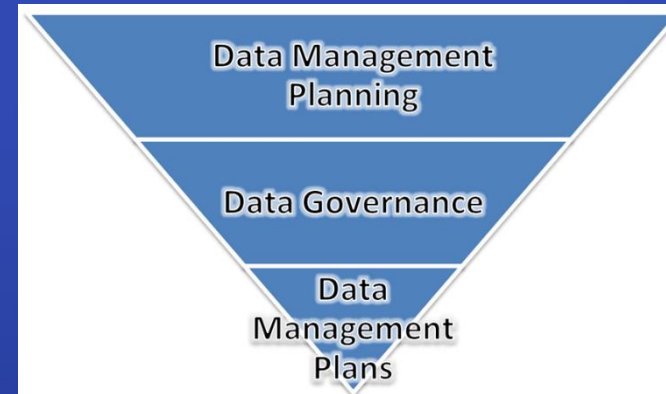
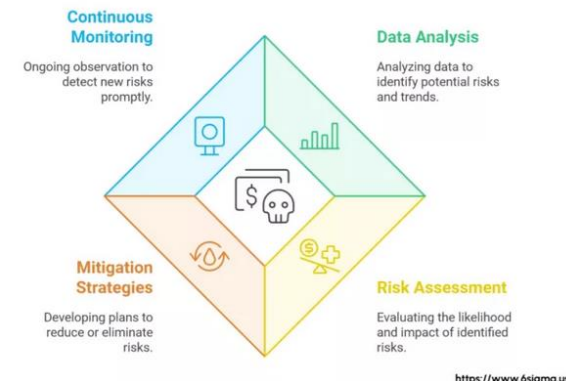


Figure 1. Relationship of data management planning components.

Risk Management Automation



Data Governance & Safe Collaboration



- Role-Based Access Control (RBAC), encryption, MFA.



- Use secure sharing protocols and federated identities.



- Avoid personal cloud tools; prefer controlled environments.

Incident Preparedness & Standards

1

Develop tailored
incident response
plans.

2

Conduct regular
tabletop exercises.

3

Align with NIST SP
800-171, ISO/IEC
27001, NIH & DoD
standards.

Role of AI & LLMs



OPPORTUNITIES:

- THREAT DETECTION AND LOG ANALYSIS.



- POLICY DRAFTING AND COMPLIANCE SUPPORT.



- CYBERSECURITY TRAINING TOOLS.



RISKS:



- DATA LEAKAGE.



- ADVERSARIAL MISUSE.

Stakeholder Responsibilities & Recommendations

Responsibilities:

- Researchers, IT/cybersecurity staff, leaders, data managers.

Recommendations:

- Continuous risk assessments.
- Cybersecurity & AI in all DMPs.
- AI governance frameworks.
- Training programs.
- AI-assisted secure repositories.

Conclusion

- Cybersecurity and AI governance are strategic necessities.

- Secure-by-design and AI-aware RDM workflows protect integrity and compliance.

- Acting proactively strengthens trust and responsible innovation.

Q & A?
smiller@whatcom.edu

