NC PEAK

Cyber Risk Management

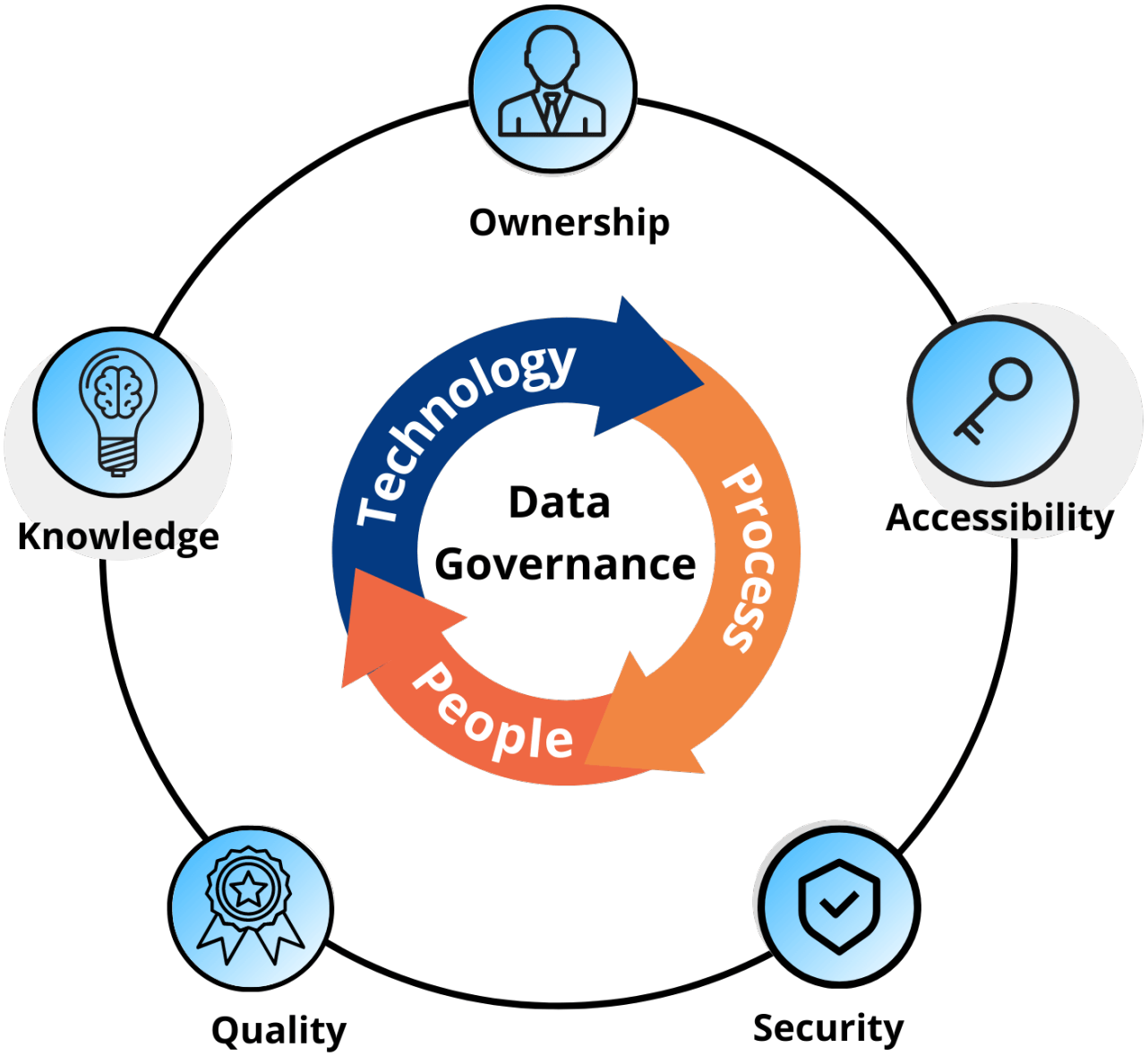
Bernice Russell-Bond

State Chief Information Security Officer

Cyber Risk Management

Data Governance

- Know the Data
  - Ownership
  - Sensitivity
  - Location



Security Review

- 3rd Party Vendor
- Security Standards
- Policy Exception

3rd Party - Security Review Purpose

In today's interconnected digital landscape, organizations increasingly rely on third-party systems and vendors to support business operations, enhance productivity, and deliver value to customers.

While these partnerships can provide critical benefits, they also introduce new risks—particularly in the realm of cybersecurity. Conducting thorough security reviews of third-party systems is essential to safeguard organizational data, maintain regulatory compliance, and protect stakeholder trust.

It helps mitigate risks, ensures compliance, supports business continuity, and builds stakeholder trust. By making security assessments a routine part of vendor management, organizations can confidently leverage external partnerships while protecting their most valuable assets

Process

- Agency CISO or Security Liaison
  - Subject matter experts to consult the requestor through the process.
    - Artifacts needed from vendor.
    - Security controls that should be in place based on data sensitivity.
  - Initial decision required prior to ESRMO review.
- ESRMO
  - Quality Assurance of review by Agency CISO/Security Liaison.
  - Decisioning prior to SCIO review.

IoT and OT Security

Internet of Things IoT - Devices are internet-connected - collect and exchange data in real time.

Operational Technology (OT) - OT devices control the physical world

The intersection of the Internet of Things (IoT) and Operational Technology (OT) represents a significant shift in the industrial landscape.

Policy / Standard Exception

- Approval is required to ensure that any deviation from established protocols is properly evaluated and justified.
- This process helps organizations assess the potential risks associated with making an exception and allows decision-makers to implement necessary safeguards or controls. By requiring approval, organizations maintain accountability, protect sensitive data, and minimize the likelihood of security breaches.

Deviation Approval

Temporary - 1 year or less for waivers

expectation is to move to compliant state

Permanent – timeframe may vary

Risk is accepted not to remediate the system

Process

- Agency CISO or Security Liaison
  - Subject matter experts to consult the requestor through the process
    - Is request for waiver justified
    - Identification and documentation of mitigation controls
  - Initial decision required prior to ESRMO review
- ESRMO
  - Quality Assurance of review by Agency CISO/Security Liaison
  - Decisioning prior to SCIO review

Process Updates

Moving security/standard exceptions out of Ariba

Communication coming about new tooling and training

3rd Party Risk Management

BitSight

GovRAMP