

Building a Cloud Security Authorization (ATO) Strategy

Presented by:

Jaime Lynn Noble, CAP, CISSP

Chief Information Security Officer
Office of Justice Programs
U.S. Department of Justice



Cloud is Here

- Cloud has become an integral part of the Enterprise
 - A catalyst for Business Innovation
 - Driving IT Modernization

\$112 Billion
Investment
In the next 5
years

Cloud is over taking
On-Premises

Changing the
IT Business

New
Skills



- Cloud Adoption Strategy
- Inform Analysis of Alternatives
- Integrate Security into IT Governance



Strategy



Alternatives
Analysis



Governance





Strategy

Organizational Risk Strategy

- Managing risk is a complex, multifaceted activity that requires the involvement of the entire agency—
 - **Senior leaders and Executives** providing the strategic vision and top-level goals and objectives for the agency;
 - **Mid-level leaders** planning, executing, and managing projects;
 - **Individuals** on the front lines operating the information systems supporting the agency's missions or business functions.





Strategy

Cloud Adoption Roadmap

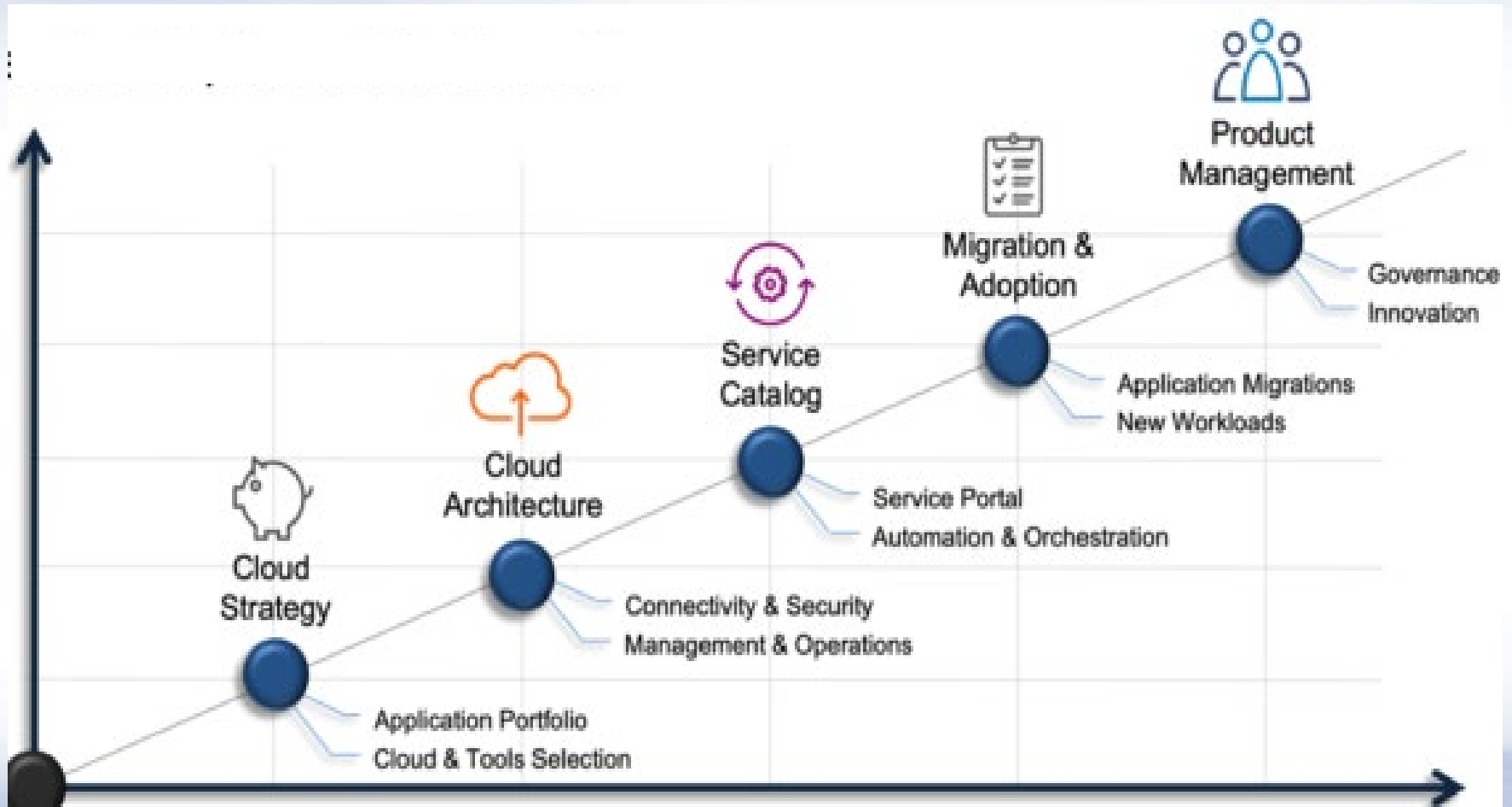
- Understand your Organization's Mission
 - Drive business value
 - Protect the mission!
- Inform Organizational Cloud Strategy
 - Budget for security
 - Schedule
 - Resources



Cloud Adoption Roadmap



Strategy





Alternatives Analysis

Inform Analysis of Alternatives

- Inform Acquisition Language
 - OMB A-130
 - FISMA requires each agency to provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, and cloud-based solutions.
 - Agency Specific clauses
 - Breach Notification Procedures
 - Disposal of Agency Information
 - FedRAMP





Alternatives Analysis

Inform Analysis of Alternatives

- All Cloud Service Providers are not equal
 - Leverage FedRAMP Market Place
 - Sponsor a CSP through FedRAMP





Governance

Integrate Information Security

- IT Investment Review Boards
- Enterprise Architecture
 - Common Technologies
 - Reduce complexity
- Systems Development Life-Cycle
 - Budget
 - Acquisitions
 - Security Requirements





Governance

Security Assessment & Authorization



Information Security Continuous Monitoring



Governance



