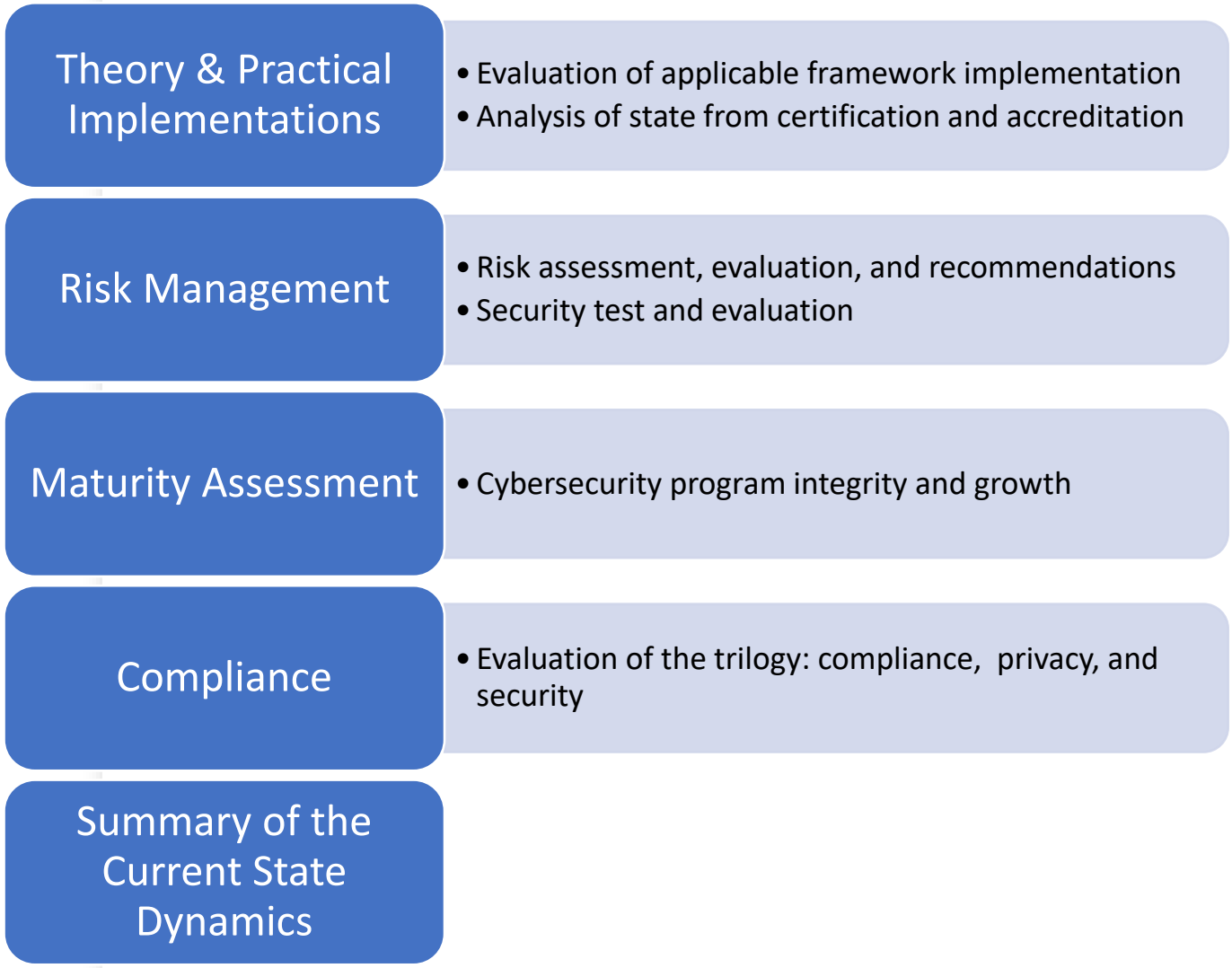
CYBERSECURITY GOVERNANCE & OPERATIONS

CAPABILITY MODELING

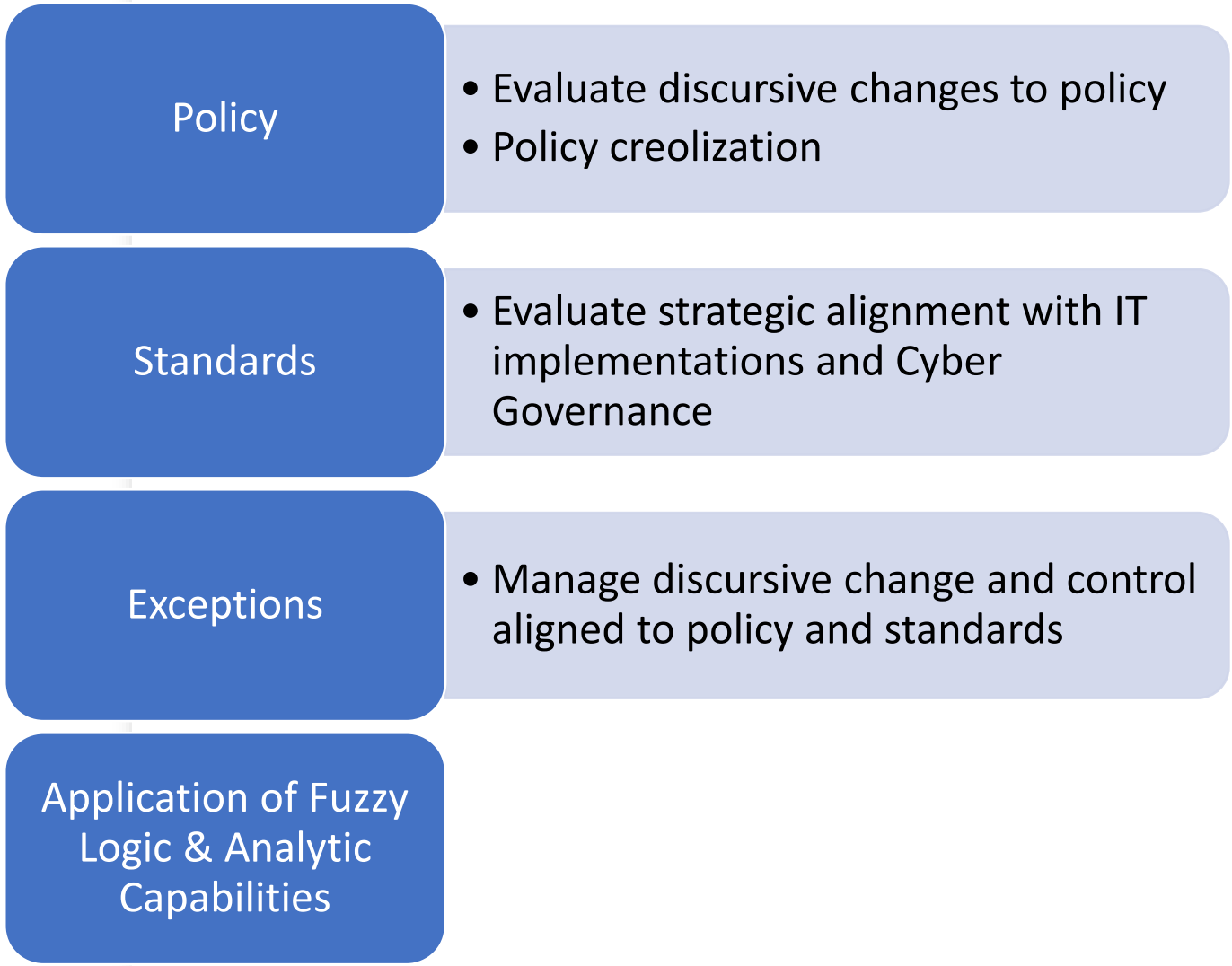
Services Overview

Governance, Risk & Compliance	• Strategic alignment of organizational goals • Gap analysis of existing enterprise dynamics
Security Program Integrity	• Policy alignment with standard implementation • Exception management and risk evaluation
Application Security & Technical Advisory	• Consensus and exploration of the business impact • Deviations from accepted organizational norms
IT Change & Metrics	• Qualitative inquiry into IT administration • Analysis of tactical and technical changes
Operational Awareness & Skills	• Skills evaluation of the “human-in-the-loop”

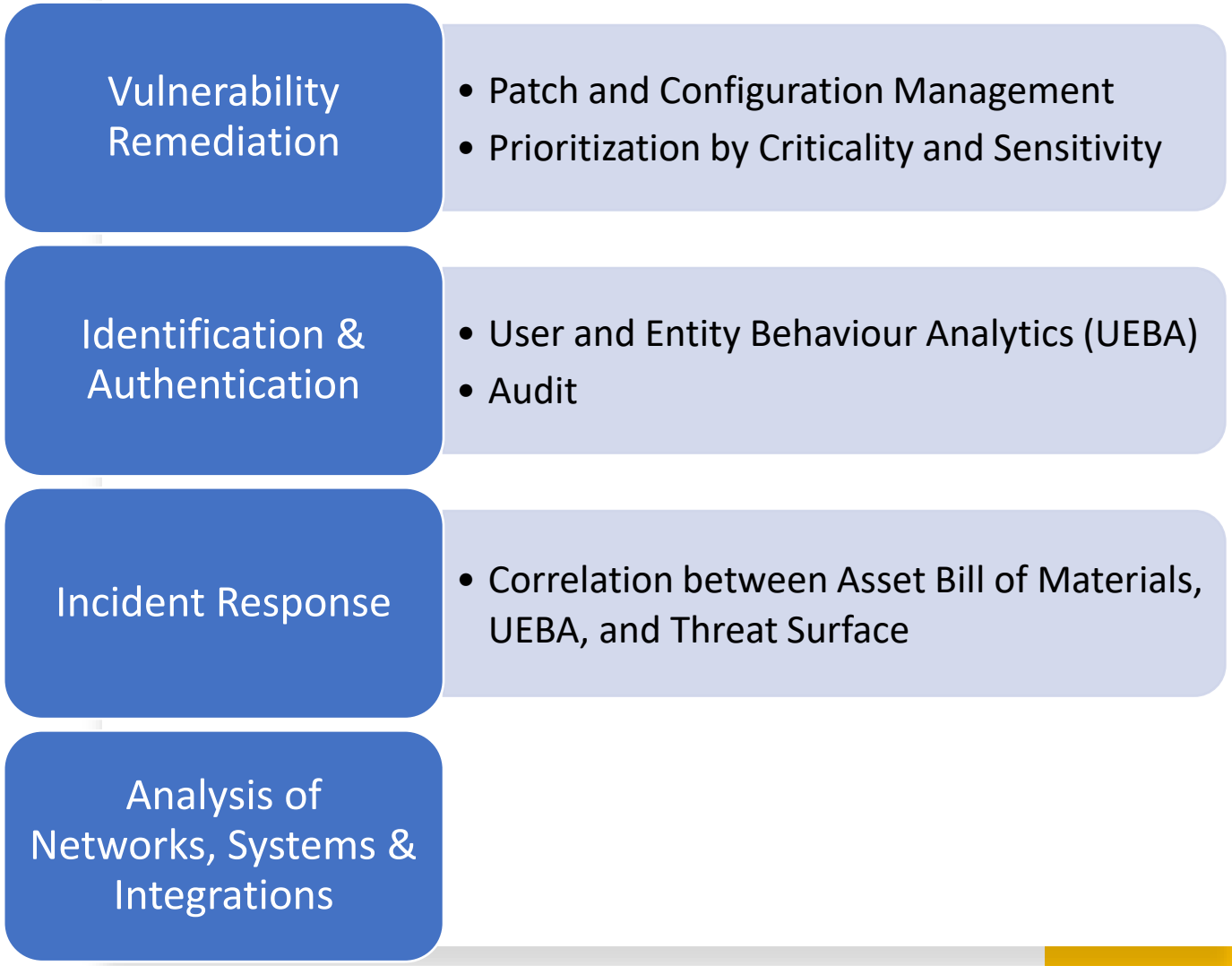
Governance Risk Compliance



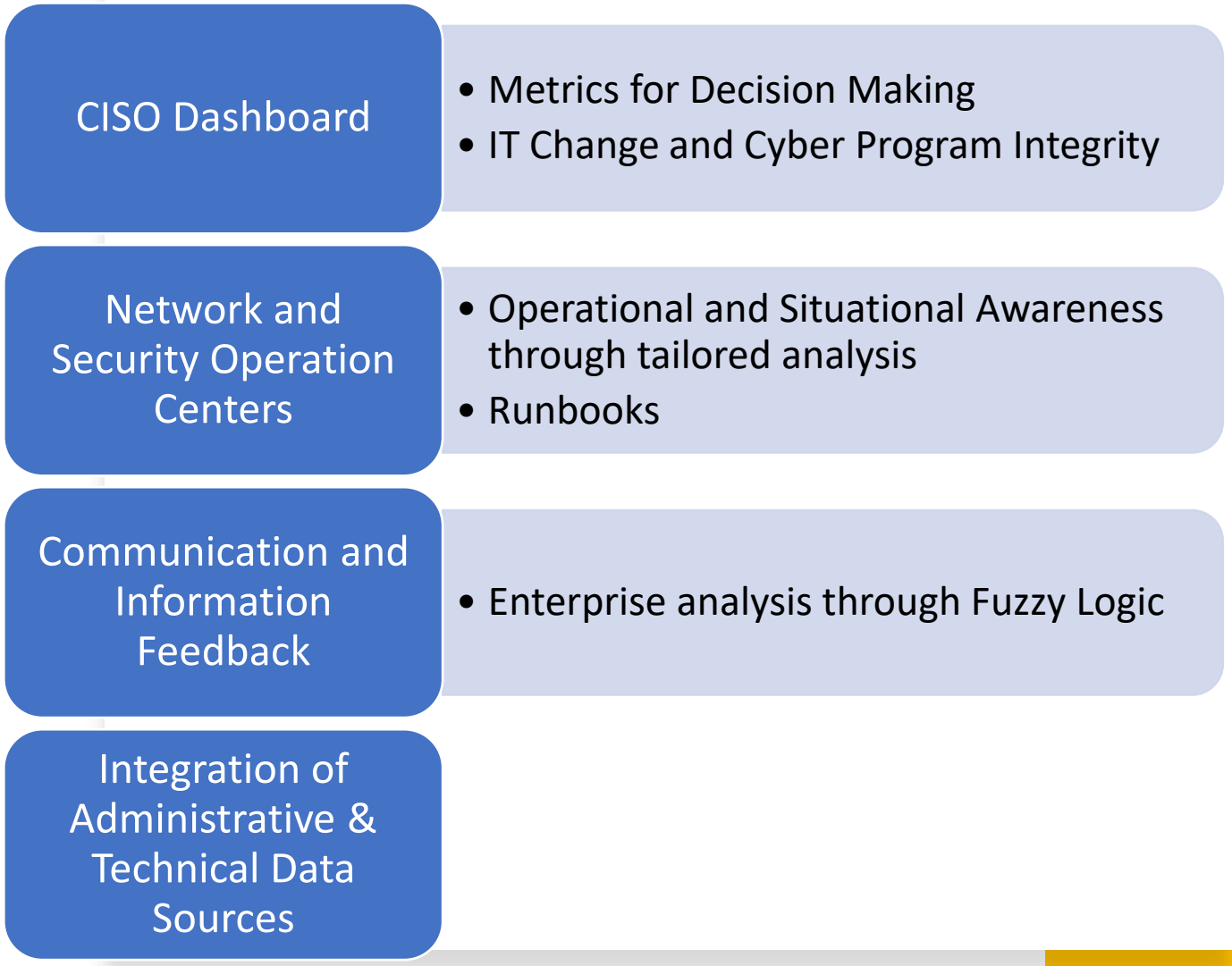
Security Program Integrity



Application Security & Technical Advisory



IT Change & Metrics



Operational Awareness & Skills

Human-In-The-Loop	• Man-Machine Analysis of Controls • Evaluation of human security operators
Knowledge, Skills & Abilities	• Measure core competencies based on job duties, operational environment, and resiliency
Balanced Scorecards	• Evaluation of risk management capabilities in context of operational environment and cyber capabilities
Attestation of the Investments in Security	

Human and Entity Relationship

The evaluation of human factor cybersecurity competency across the dynamic systems integrating functional departments support understanding the contextual environment and inherent risks.

The Duality of Cybersecurity Risk