

Controlled Unclassified Information FRAMEWORK

Cybersecurity Research Data Framework

Purdue RCAC Jessica Ackerman, Benjamin Cook, Ziyang Tang

Problem

- Researchers left to fend for their own cybersecurity options, often leading to poor choices out of ignorance or neglect or unforeseen costs
- Purdue loses opportunities for research as a result

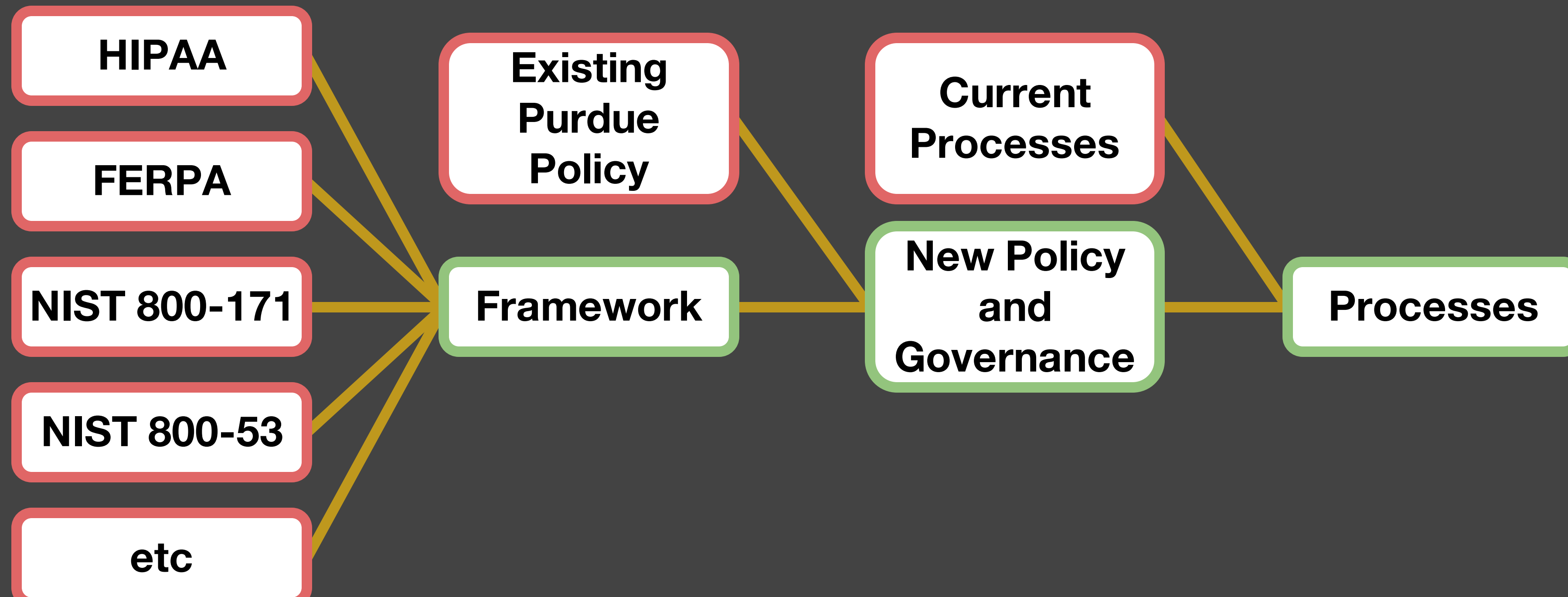


Solution

- Create a framework that guides researchers in the safe practices of managing their research data, covering all possible data types

Methods

- Analyzing the many data types researchers use such as HIPAA, FERPA, NIST 800-171 and NIST 800-53 CUI, etc
- Constructing a Framework that includes the restrictions and compliance for all of the data types under one Framework
- Designing the process for implementing this throughout the different regulatory offices



Student Experiences

- Experience with the various forms of Compliance
- Producing Tabletop Exercises for our SOC team
- Exposure to the modification of existing systems and policies

Results

- Better practices, leading to meeting compliance for the needed data types
- Reduces risk of data breaches and compliance violations
- Leads to creating an environment where Purdue gains additional research opportunities, they were not previously capable of.
- This is a common problem among other universities as well, so the goal is to build the framework such that it can be applied at any university