### **Classroom Activity: AI-Enabled Security Assessment of a Hypothetical Company**

**Overview:**In this activity, students will review a description of a hypothetical company and their current state for a particular security domain and related controls and processes, against the NIST 800-53 Revision 5 (r5) framework, to assess a company’s control environment, identifying control gaps and making recommendations for remediation. First, students will conduct this assessment manually, using only the available documentation, then they will utilize AI to assist with the same assessment. By comparing the two approaches, students will gain insight into the effectiveness of leveraging AI in benchmarking unstructured, qualitative data against a complex security framework like NIST 800-53 (r5), and how this could be applied in the real world today.

**Activity:**

* First, your team will review a detailed description of one of four fictional companies (MediVault Health, AeroSync Technologies, TerraBloom Solutions, and LuminoGen) against the full NIST 800-53 r5 framework, attempting to manually identify control gaps and recommendations based on the available information.
* Second, your team will run an AI solution capable of natural language processing and qualitative analysis, in this case, Anthropic’s Claude AI, against the same information to generate control gaps and recommendations.
* Third, each team will present briefly (5 mins each) on their results from the two approaches, how they compare, the potential benefits and/or drawbacks to each, and how this could be leveraged in real life.