

## Prompt

As you prepare future class quizzes and exams, "you may want to remember" how to quantify risks as described in class. You may note that these formulations closely track the elements in the slide "Residual Risk - Consider the Effect of Controls" from the materials. Thinking up your own control and filling out the table on that slide is a good way to prepare for your post.

Read the BigU IAM introduction - also linked from the BigU case materials page. We will talk more about IAM risks later in the term. This document likely includes unfamiliar concepts and terminology. You don't need to master IAM yet! just work with what you understand so far.

Make up a risk and quantify a risk exposure that is somewhat related to the IAM controls at BigU. There is no need to spend extra time researching - you may speculate and make up details. But DO use risk terminology from the class. Provide enough (made up) details for a reader to easily understand how the computations were made. Hint exposure = [vocabulary term] \* [vocabulary term] and you need to include a time frame. Name and briefly define the vocabulary terms.

Name (make up) and provide/compute costs for a control that addresses the risk. Include both start up cost and annual costs.

Provide (make up!) up a residual exposure amount, show how it was computed. Briefly explain what it means that this amount is a residual exposure. Hint: the meaning of "residual" in this context should be clear and should be reflected in the computations you show. Which part(s) of the risk quantification are reduced by the control?

In this hypothetical scenario, BigU has recently joined the cryptocurrency trend by creating its own digital currency, BeaverCoin. Since this trend and currency are brand new, all of BeaverCoin is currently stored on a single central computer, and all affiliated computers are used for mining. This setup presents a high risk due to the centralization of the currency on one computer, especially considering the presence of ambitious cybersecurity majors who might attempt significant actions. Assuming the likelihood of a security breach is 30% and the impact of such a breach is \$500,000, the initial risk exposure is calculated as follows:

Initial Risk Exposure = Likelihood \* Impact =  $0.3 * 500,000 = \$150,000$  per year

To mitigate this risk, a proposed control involves implementing blockchain technology across all BigU-associated machines. This decentralized approach would enhance security by distributing the storage, mining processes, and record-keeping across all machines, thereby reducing the vulnerability from a single point of failure. The startup cost for this control is estimated at \$200,000, with annual maintenance costs of \$50,000. After implementing the control, the residual likelihood of a breach could drop to 5%, and the impact stays at \$500,000 as the same crypto being stolen would have the same amount of impact to BigU. The residual exposure is then calculated as follows:

Residual Exposure = Residual Likelihood \* Impact =  $0.05 * 500,000 = \$25,000$  per year

This residual exposure represents the remaining risk after the control has been applied. It shows that the control has significantly reduced the likelihood of a potential breach, thereby lowering the overall risk exposure from \$150,000 to \$25,000 per year. This is after BigU paying the \$200,000 for upgrading their systems with an additional \$50,000 per year for maintenance.