Plumcot

How a Healthcare Payor Built Enterprise Risk Assessment Capability In-House

From $300K annual consulting engagements to quarterly assessments with Plumcot and Copilot

A new regulatory requirement dropped. The VP of GRC knew how it will play out.

Another $300K check to a Big 4 firm. Another 2-month engagement. Another report that would be stale by the time it landed on the CISO's desk.

They had done enterprise risk assessments before. But never on their own. The institutional knowledge of how to run one lived at their consulting partner. Not inside their walls.

This year was different.

The Directive

The CISO laid it out: run it through Copilot this time. Two Goals:

One, increase frequency. Instead of annual assessments, do them quarterly.

Two, cut costs. Stop writing six-figure checks for work that should be a core capability.

This became one of the GRC team's AI priorities for the year.

What We Built

An AI Risk Analyst that could run the full Enterprise Risk Assessment working with the human Risk Analyst.

Here is what it handled:

- Setting up the enterprise risk survey
- Analyzing survey responses across the organization
- Identifying the top 10 risk scenarios
- Identifying controls using ATT&CK MITRE, mapping these controls to NIST CSF 2.0 and 800-53

- Analyzing the effectiveness of existing controls using evidences, interviews, and other telemetry
- Quantifying residual risk for each scenario
- Recommending remediations
- Generating the final risk assessment report for different stakeholders

The human risk analyst guided and validated at each step. AI did the heavy lifting. The analyst made the judgment calls.

90% complete analysis by AI. Final decision by human.

The Workflow

How is an Enterprise Risk Assessment exercise run?

You send out a survey. Run interviews. Review documents. Apply threat intelligence. Consider benchmarking. Identify risks. Collect evidences. Look at any real time telemetry. Analyze them. Talk to control owners. Synthesize the findings. Generate the report.

That is what consultants handle for you. That is what you are actually paying $300K for.

We built that into the workflow too.

The Outcome

50-60 hrs	2 weeks	Quarterly
HUMAN WORK	NOT 2 MONTHS	NOT ANNUAL

A complete enterprise risk assessment report. Top 10 scenarios identified. Residual risk quantified. Remediations recommended. Stakeholder reports generated.

The VP of GRC was happy. The CISO was happier.

What Happens Next

They are planning to run it quarterly now.

Using their existing Microsoft Copilot licenses. The capability lives in-house. The annual $300K check is gone.

> *"We went from paying consultants to tell us what our risks are once a year, to knowing our risk posture whenever we need to. That is not a cost savings. That is a capability we never had."*

The Point

AI has given your team capabilities that you had it to buy from consultants for years.

You need to decide what you want to do with it.

Your Next Assessment Is Coming

You know the drill. The RFP. The SOW. The six-figure invoice. It does not have to be that way.

Book a Call

30 minutes. Your GRC team, your assessment needs, what is possible.

Plumcot

plumcot.ai · pgoyal@plumcot.ai