A Better ROI for Quantifying Risk

Cost of Hiring an In-House Cyber Risk Quantification Analyst

Role profile (what you actually have to hire)

Market postings show that **true cyber risk quantification capability** (FAIR, scenario modeling, Monte Carlo, executive reporting) sits well above a general GRC analyst role.

Recent US job postings for **Cyber Risk Quantification Engineer / Analyst** explicitly include:

- FAIR methodology
- Quantitative modeling
- Scenario analysis
- Executive / board reporting
- 8–10+ years experience [clearancejobs.com], [careerbuilder.com], [theladders.com]

Base salary (US market)

- **Mid–senior CRQ analyst**:
  $120K–$160K base salary
- **Senior / engineer-level quantification specialist**:
  $165K–$260K base salary [clearancejobs.com], [careerbuilder.com]

Fully loaded employer cost

Once you include benefits and overhead (HR, tooling, management, time to ramp), a conservative multiplier of **1.25–1.4× salary** is standard.

Level	Base Salary	Fully Loaded Annual Cost
Mid-level CRQ Analyst	$130K	~$162K–$182K
Senior CRQ Engineer	$200K	~$250K–$280K

(Benefit load assumptions: 25–40%, consistent with US corporate norms; salary ranges sourced above)

What this *still does not* buy you

Even with a strong hire:

- Quantification coverage is **limited by analyst bandwidth**
- Scenario modeling quality depends heavily on **organizational data maturity**
- Executive-ready outputs often require **review cycles and iteration**
- Turnover risk resets institutional knowledge

This explains why many firms with in-house analysts still supplement with consulting.

Cost of Hiring a Firm to Quantify the Risk of **One Scenario**

> **Important**: Major firms (PwC, KPMG, Marsh) do **not publish per-scenario prices**. However, their own methodology descriptions allow us to infer pricing *structure*, not just guess numbers.

How consulting firms scope CRQ work

Sources from Marsh, KPMG, PwC confirm:

- Work is **scenario-based**
- Uses Monte Carlo / loss exceedance modeling
- Designed for **board-level financial decision-making**
- Typically packaged as a **project**, not hourly staff aug [corporate.marsh.com], [kpmg.com], [pwc.com]

Typical engagement shape (explicitly described)

- Scenario definition & scoping
- Threat + control assumptions
- Frequency & impact modeling
- Financial loss distribution
- Executive report / board discussion

This is consistent across Big 4 and specialist CRQ firms.

Cost range: single-scenario quantification (US market)

Based on:

- Published consulting fee models (project-based vs hourly) [consulting...uccess.com]
- Scope descriptions from PwC / KPMG / Marsh (scenario-based quantitative modeling) [corporate.marsh.com], [kpmg.com], [pwc.com]
- Typical senior consultant billing models (implied, **not numerically published**)

Observed market ranges:

Engagement Type	Typical Cost (USD)
Lightweight single-scenario (internal workshop + model)	**$15K–$30K**
Standard single-scenario quantification (FAIR-based, board-ready)	**$30K–$60K**
Big 4 / global firm, single scenario	**$50K–$100K+**

Why such variance?

- Brand premium (Big 4 vs boutique)
- Depth of data collection
- Governance defensibility (audit / insurance use)
- Custom executive reporting

⚠️ None of these firms price "per Monte Carlo run" or "per spreadsheet." Pricing is **value- and defensibility-based**, not effort-based.

Direct Comparison: In-House vs Single-Scenario Consulting

Option	Annualized Cost	Pros	Constraints
In-house analyst	$160K–$280K/year	Ongoing capability, internal knowledge	Fixed cost, limited throughput
Consulting – 1 scenario	$30K–$60K	Fast, defensible, board-ready	One-off, not reusable internally
Consulting – Big 4	$50K–$100K+	Brand leverage, audit-ready	Cost, slower iteration

Why this cost structure matters (exec lens)

From PwC and Marsh research:

- Boards struggle with **qualitative cyber risk**
- Quantified scenarios enable **insurance, investment, and appetite decisions**
- But **cost and scalability remain adoption barriers**, especially below 10,000 employees [corporate.marsh.com], [pwc.com]

This creates the exact gap you're working in:

- Too expensive to staff full-time
- Too expensive to hire consultants per scenario
- Yet executives still need **financially expressed cyber risk**

Stop Paying Six Figures to Answer One Question

Subscribe to *The Cyber Risk Forecast*

Most organizations face the same choice:

- Hire a $200K+ analyst to model cyber risk internally, **or**
- Pay $30–$60K every time they need a single quantified scenario.

The Cyber Risk Forecast gives you a third option.

Each month, you get:

- **Quantified cyber risk scenarios**, expressed in financial terms
- **Industry-specific loss ranges** executives can actually use
- **Forward-looking risk signals** based on current attacks—not last year's reports
- **Board-ready insight** without weeks of analysis or consulting fees

No new headcount.
No six-figure engagements.
No vague "high / medium / low" risk ratings.

Just clear, defensible cyber risk intelligence—delivered on a subscription.

👉 **Subscribe to The Cyber Risk Forecast** and start making cyber risk decisions at the speed and cost the business expects.
