

Birdseye Quantify: Quantify Risk Your Way

Leverage the full FAIR™ ontology with no usage restrictions to simulate risk scenarios.

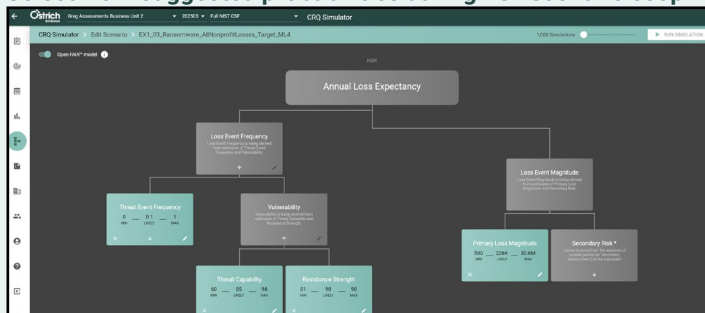
A SaaS solution that gives you control to scope, build and simulate risk scenarios without limiting the way you can use the FAIR model or the complexity of the scenarios you build.

Why Birdseye: What Makes Birdseye Quantify Different than other CRQ Solutions

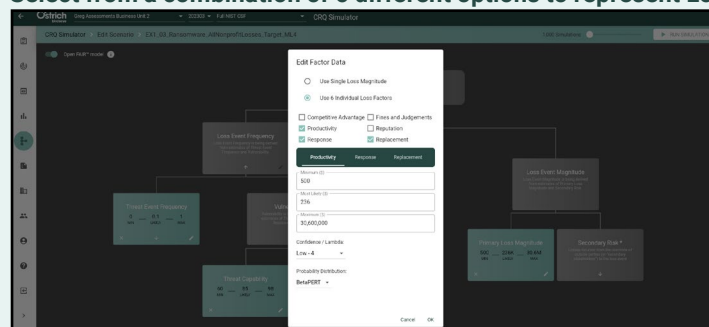
- 1. Ease of Use:** Use the full FAIR™ ontology to create unlimited risk scenarios
- 2. Annual Loss Expectancy (ALE) Comparison:** Analyze scenario results to determine best ROI
- 3. Leverage Industry Data:** Take advantage of suggested Loss Event Frequency and Primary Loss Magnitude probabilities in your scenarios calculated by your industry's historic loss claims
- 4. Guided Threat Scenario Definition:** Build and customize scenarios using a guided threat scenario definition scoping wizard
- 5. Customer Success:** 1:1 customer meetings for onboarding, technical support and quarterly business and product updates
- 6. Get the Right Support:** Optional Professional Services are available to meet you where you are in your CRQ journey with introductory help in CRQ or expert advice for your CRQ program

Birdseye CRQ Simulator

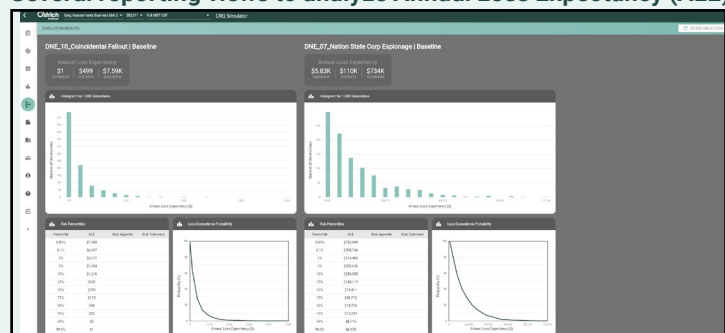
Select from suggested probabilities during risk scenario scoping



Select from a combination of 6 different options to represent Loss Event Magnitude






Several reporting views to analyze Annual Loss Expectancy (ALE)



How Birdseye Quantify Works

Enhanced by Birdseye Analytics

Benchmark scenario inputs according to industry segment and organization size.



-  Integration to Advisen™ curated historic loss claims data by industry
-  Run deterministic models to suggest FAIR risk factor values for Loss Event Frequency & Loss Event Magnitude
-  Benchmark your risk scenario simulation results against your industry's Annual Loss Expectancy (ALE)

Birdseye CRQ Context Manager

Save time building scenarios with a guided scenario definition and scoping wizard.

THREAT DRIVER(S)		SUSCEPTIBILITY FACTORS			
Threat Community:	Hacktivists: Coordinated Unaffiliated Groups		Key TTPS (MITRE)	Persistence	Impact
			Key Vulnerabilities:		Discovery
Motive:	Financial: Extortion	Thematic: ESG	Key Surface Prevention Controls:		Persistence
Target Criteria:		Thematic: Patriotic	Key Surface Removal Controls:		Resource Development
Starting Access:		Financial: Data Sale	Key Exploit Prevention Controls:		Reconnaissance
		Financial: Extortion	Key Exploit Response Controls:		Collection

Features:

-  Out-of-the-box library of common risk scenario families that can be used to start your CRQ journey
-  Build specific scenarios under a default scenario family, or create a new scenario family

Build Trust in the Process:

-  **1** Certainty
-  **2** Objectivity
-  **3** Tangibility
-  **4** Communicability
-  **5** Consensus
-  **6** Transparency

CRQ Professional Services

Available for Birdseye customers who want help to build out their CRQ program, or further refine risk quantification by implementing CRQ best practices for better outcomes.



CISO/CIO/CRO

- CRQ Program Strategy
- Customized CRQ Program Framework
- Change Support



Risk Manager /Analyst

- Getting started with CRQ
- Common pitfalls
- Risk scenario scoping expert advice



To learn more about other Ostrich Cyber-Risk offerings, visit www.ostrichcyber-risk.com or contact info@ostrichcyber-risk.com