Buyer's Guide: Cloud Risk Analytics

Running your risk applications on a cloud-native platform or cloud-hosted environment is critical to the long-term success of your underwriting, portfolio management and regulatory reporting disciplines. When evaluating potential solutions, it's important to ask questions about the Risk Fundamentals, the Data Management Capabilities and the Platform Services, of each environment.

TOP QUESTIONS TO CONSIDER	WHAT TO ASK	PITFALLS OF CLOUD-HOSTED ENVIRONMENTS
	RISK FUNDAMENTALS	
1	**FINANCIAL MODELING** Do your applications share the same financial engines?	Financial results across applications may be materially different without precise, transparent guidance on why.
2	**GEOCODING** Does your environment provide consistent geocoding across applications?	Cloud-hosted applications may use third-party or different geocoding engines.
3	**REAL-TIME DATA INTEGRATION** Does your application support near-real-time visualization and accumulation analytics?	Some cloud-hosted applications may require you to manually upload real-time event data and forecasting into the accumulation analyses.
4	**THIRD-PARTY MODELING** Can your applications run your home-grown models or models from multiple vendors?	Most cloud-hosted applications can only run their own proprietary models.
5	**MODELING FLEXIBILITY** Can you run 3rd party models natively within or outside your environment?	Most cloud-hosted applications cannot support either deployment option for 3rd party modeling.
	DATA MANAGEMENT	
6	**EXPOSURE DATA** Do your applications share the same exposure data?	Cloud-hosted solutions may run in different data centers using inconsistent datasets.
7	**DATA AVAILABILITY** Can your model applications access, analyze, and edit data stored in on-premises data centers and data stored in the cloud?	Cloud-hosted solutions may require you to migrate all your exposure data to the environments before running your applications.

Buyer's Guide: Cloud Risk Analytics

TOP QUESTIONS TO CONSIDER	WHAT TO ASK	PITFALLS OF CLOUD-HOSTED ENVIRONMENTS
	DATA MANAGEMENT, CONT'D	
8	**DATA BACKUP** What is your policy for production data backup and disaster recovery?	Cloud-hosted solutions may not follow industry best practices for data backup and disaster recovery.
9	**DATA SCHEMA** Can your applications ingest, store, and analyze multiple data schemas, such as CEDE and OED?	Most cloud-hosted applications can only analyze a single data schema.
	PLATFORM SERVICES	
10	**APIs** Can you import and export data using public REST APIs across applications?	Cloud-hosted solutions may require custom code to move data across systems.
11	**USER AUTHENTICATION** Does your environment integrate with single sign-on (SSO) such as Microsoft Active Directory, Okta, or PingFederate.	Vendors may utilize their own security frameworks, which is unable to integrate with enterprise security frameworks.
12	**ROLE-BASED ACCESS CONTROLS** Does your platform maintain user-permissions across applications?	Vendors may require you to create unique credentials for each application.
13	**SOFTWARE PATCHING AND UPDATES** How does your platform manage software patches and security updates?	Cloud-hosted solutions may require your IT team to update and manage software patches in your environment.
14	**APPLICATION AVAILABILITY** Are applications on your environment available 24-7?	Cloud-hosted solutions may not offer automated failover across the different environments.
15	**SCALABILITY/RELIABILITY** Does your environment seamlessly scale based on the number of users and activities?	Cloud-hosted environments may lack the processing power to meet your workload needs during critical periods, such as renewals.