RMS A Moody's Analytics Company

Buyer's Guide: Cloud Risk Analytics

Running your risk applications on a cloud-native platform or cloud-enabled 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-ENABLED 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-enabled 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-enabled applications may require you to manually upload real-time event data and forecasting into the accumulation analyses.
	DATA MANAGEMENT	
4	**EXPOSURE DATA** Do your applications share the same exposure data?	Cloud-enabled solutions may run in different data centers using inconsistent datasets.
5	**DATA AVAILABILITY** Can your model applications access, analyze, and edit data stored in on-premises data centers and data stored in the cloud?	Cloud-enabled solutions may require you to migrate all your exposure data to the environments before running your applications.
6	**DATA BACKUP** What is your policy for production data backup and disaster recovery?	Cloud-enabled solutions may not follow industry best practices for data backup and disaster recovery.

RMS A Moody's Analytics Company

Buyer's Guide: Cloud Risk Analytics

TOP QUESTIONS TO CONSIDER	WHAT TO ASK	PITFALLS OF CLOUD-ENABLED ENVIRONMENTS
	PLATFORM SERVICES	
7	**APIs** Can you import and export data using public REST APIs across applications?	Cloud-enabled solutions may require custom code to move data across systems.
8	**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.
9	**ROLE-BASED ACCESS CONTROLS** Does your platform maintain user-permissions across applications?	Vendors may require you to create unique credentials for each application.
10	**SOFTWARE PATCHING AND UPDATES** How does your platform manage software patches and security updates?	Cloud-enabled solutions may require your IT team to update and manage software patches in your environment.
11	**APPLICATION AVAILABILITY** Are applications on your environment available 24-7?	Cloud-enabled solutions may not offer automated failover across the different environments.
12	**SCALABILITY/RELIABILITY** Does your environment seamlessly scale based on the number of users and activities?	Cloud-enabled environments may lack the processing power to meet your workload needs during critical periods, such as renewals.