MOODY'S | RMS

RiskLink® vs. Risk Modeler™ Model Change Management

What's involved in validating catastrophe models with your own IT environment? You and your team are responsible for managing your on-premises modeling solutions — including installing the new testing environment and handling all the data. As you consider the time and effort required to update a new model, the table below offers a brief comparison of the differences between model change management with on-premises RiskLink software and with Risk Modeler, our cloud-native, catastrophe modeling application hosted on the Moody's RMS™ Intelligent Risk Platform™.

ESSENTIAL STEPS	RISKLINK ON-PREMISES ENVIRONMENT	RISK MODELER CLOUD ENVIRONMENT
1 IT PLANNING AND PROCUREMENT FOR NEW ENVIRONMENT	Long IT budgeting, procurement, and planning process.	No additional IT procurement needed.
2 NEW ENVIRONMENT PROVISIONING	IT maintains multiple environments and the accompanying software.	Change management runs on existing cloud-native environment.
3 UPDATE SYSTEM REQUIREMENTS	IT conducts review of new system requirements, which can include security and compliance audits.	Software-as-a-service (SaaS) modeling approach keeps workflow software up to date.
4 MODEL SOFTWARE INSTALLATION AND MAINTENANCE	IT downloads and installs model software in new environment. Monitors and maintains both versions during change management.	New model becomes instantly available. No new software installation needed.
5 PORTFOLIO DATA MIGRATION	Duplicate and migrate live exposure data to new testing environment.	No data migration needed. New and existing models share the same exposure data for analysis.
6 WORKFLOW INTEGRATION	IT builds new workflows that feed into existing systems.	Leverage existing workflows from production environment.
7 PORTFOLIO ANALYSIS AND MODEL VALIDATION	Model runs can take days or weeks to complete.	Risk Modeler can run models up to 10 times faster than RiskLink.
8 POST MODEL VALIDATION	Maintain new and old production environments. Customer data remains on both systems.	Customer data remains secure in unified data store.