

Article Title: ARCHIVE | Criteria | Insurance | General: Summary Of Recent Enhancements To Insurer Enterprise Risk Management Criteria Data: (EDITOR'S NOTE: —This article is no longer current. It has been superseded by "Insurance Criteria: Refining The Focus Of Insurer Enterprise Risk Management Criteria," published June 2, 2006.) In October 2005, Standard & Poor's Ratings Services introduced a set of criteria for our insurance analysts to use to rate enterprise risk management (ERM) at insurance companies. Since then, we have been using this criteria set to evaluate ERM quality at insurers and incorporating that information into our counterparty credit and financial strength ratings. With information gathered from those evaluations, we are publishing an extensive enhancement of the criteria. We also made some major additions and revisions, and we have clarified what these criteria are meant to be and what they are not. In a nutshell, these criteria are not intended as a roadmap for insurers to use to organize their ERM. Rather, the criteria describe how Standard & Poor's will analyze ERM in our rating process. Where ERM is performed—by a central ERM-dedicated unit, a business risk management unit, in functional units that cross businesses, by other corporate or business unit staff, or through outsourcing—is not material to the rating. What is material is seeing an insurer performing all of the important risk management functions in an effective manner, with working checks and balances. Lastly, we do not see these criteria as being a complete set of risk management practices but rather an extensive explication of sound practices. Not all of these practices are necessary for all insurers, nor are all of these practices sufficient to control adequately all of the risks of any insurer. ERM should be a way for an insurer's management team to determine whether its risk management practices are sufficient to manage its risks, given its situation and company structure.

**Definitions Refined** We have refined our ERM quality definitions: A Weak ERM rating means an insurer lacks or has incomplete control systems for one or more important risks. An Adequate ERM rating reflects a competent, traditional, silo type of risk management program for controlling an insurer's most important risks. A Strong ERM rating means the insurer has all the characteristics of an Adequate rating but also has risk-control practices that exceed the adequate level for its major risks. In addition, it has a well-developed overall view of risks, with the view of making risk/reward trade-offs among the risks, and it has a process for anticipating emerging risks. An Excellent ERM rating would go to insurers that have all the characteristics of a Strong ERM company and are more advanced in the development of the processes, in implementation, or in effectiveness of execution.

**Risk Management Culture** Because ERM's purpose is to optimize returns for risks taken in an insurer's risk tolerance, insurers would need to have fully articulated risk tolerance. Risk tolerance is a numerical expression of maximum acceptable losses at a defined confidence interval or frequency, and it is based on a company's risk appetite. Risk appetite is a statement of the broad range of loss outcomes or consequences that would be acceptable to management. The criteria also list the need for risk preferences, which are additional statements that clarify an insurer's approach to many aspects of risk not expressed in a single loss value. Standard & Poor's looks for insurers to have articulated these ideas and communicated them appropriately inside and outside their operations. We will also look to tie directly an insurer's formation of risk limits with its risk tolerances as a part of our evaluation of risk management culture. In addition, the risk management culture evaluation will reflect the insurer's general quality of governance.

**Risk Controls** A wide range of sound practices exist for controlling risks. Those practices let an insurer identify and monitor risks, set standards and limits for the risks, enforce those standards, manage the risks, and learn from their ongoing risk management and loss experiences. Standard & Poor's will evaluate whether an insurer's selected practices for controlling each major risk accomplish those objectives. Extensive examples are outlined for risk control for credit and counterparty risk, interest rate risk, equity risk, nonlife insurance risk, life insurance risk, new product risk, and operational risks. Examples of particular practices for each risk that we find favorable to our opinion of risk control quality are also provided. We will also give full consideration to innovative techniques not documented here, if those techniques enable sound practice. In addition, some insurers might have important risks not included in this material. We expect to discuss these risks with insurers that take them and will look to find risk-control practices that fulfill the generally defined characteristics.

**Emerging Risks** The emerging risk management criteria section was formerly titled extreme event risk management. Its focus is on assessing the processes insurers use to imagine, track, prepare for, and learn from new risks that could emerge. The underwriting risk associated with a potential catastrophe should be analyzed as part of an insurer's risk-control

processes and risk models, whereas a catastrophe's potential operational impact (e.g., if an event affects a company's premises) should be dealt with under business continuity as an operational risk.

**Risk Models** Risk model evaluation will focus on the quality of processes that support the models used to provide risk information. The review will assess the underlying methodologies and principles that model a company's processes and controls to ensure that timely, accurate, and complete data is used by the models, ensure that the assumptions used are robust and appropriate, and ensure that the insurer has an adequate process for updating the assumptions. We will also review an insurer's process for running, maintaining, validating, and checking its models. Finally, we will review the number and qualifications of those individuals involved in the modeling process, whether internal or external. This list would form an outline of an extensive audit of an insurer's risk modeling, but we only intend to hold brief discussions with insurers on each of these topics or receive existing documentation if available. Information detailing how Standard & Poor's will make ERM quality decisions in each of these areas is provided in the full document.