June 2017

Principles for Fair and Accurate Security Ratings

As security ratings continue to mature, more organizations in the public and private sectors leverage them in making business and risk decisions. As a key piece of a robust security evaluation program, security ratings based on accurate and relevant information are useful tools in evaluating cyber risk and facilitating collaborative, risk-based conversations between organizations. Security rating companies use a combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate an organization's security effectiveness into a quantifiable measure or score. As these ratings rely in part upon the quality and breadth of the data they use, the variety of sources and the dynamic nature of the environment create risks of producing ratings that can potentially be inaccurate, irrelevant or incomplete. To increase confidence in security ratings, an industry-wide, common approach should:

- Promote quality and accuracy in the production of security ratings
- Promote fairness in reporting
- Include a coordinated process for adjudicating errors or inaccuracies in reported content
- Establish guidelines for appropriate use and disclosure of the scores and ratings

We believe these principles will promote fairness in reporting and enhance the value of security ratings across all industries.

Transparency: Rating companies shall provide sufficient transparency into the methodologies and types of data used to determine their ratings, including information on data origination as requested and when feasible, for customers and rated organizations to understand how ratings are derived. Any rated organization shall be allowed access to their individual rating and the data that impacts a change in their rating.

Dispute, Correction and Appeal: Rated organizations shall have the right to challenge their rating and provide corrected or clarifying data. Rating companies should have an appeal and dispute resolution process. Disputed ratings should be notated as such until resolved.

Accuracy and Validation: Ratings should be empirical, data-driven, or notated as expert opinion. Rating companies should provide validation of their rating methodologies and historical performance of their models. Ratings shall promptly reflect the inclusion of corrected information upon validation.

Model Governance: Prior to making changes to their methodologies and/or data sets, rating companies shall provide reasonable notice to their customers and clearly communicate how announced changes may impact existing ratings.

Independence: Commercial agreements, or the lack thereof, with rating companies shall not have direct impact on an organization's rating; any rated organization will be able to see and challenge their rating irrespective of whether they are a customer of the rating company.

Confidentiality: Information disclosed by a rated organization during the course of a challenged rating or dispute shall be appropriately protected. Rating companies should not publicize an individual organization's rating. Rating companies shall not provide third parties with sensitive or confidential information on rated organizations that could lead directly to system compromise.

The following organizations are supportive of the principles for fair and accurate security ratings. Support for these principles should not be construed as an endorsement of a particular company or methodology.

AbbVie
AES Corp.
Aetna
American Express
Bank of America
Bank of New York Mellon
BitSight
Blackstone
BT
Charles Schwab
Chevron
Cisco
Citigroup
ClearForce
ClearSky
CyberGRX
Dealogic
Eli Lilly
E*TRADE
Fannie Mae
FICO
Goldman Sachs
The Home Depot
Honeywell International
JPMorgan Chase & Co.
Lockheed Martin
Microsoft
Morgan Stanley
NTT
Rackspace
Raymond James Financial
Raytheon
RiskRecon
Schlumberger
Securities Industry and Financial Markets Association (SIFMA)
Security Scorecard
Starbucks
State Street
TIAA
U.S. Bank
Verizon
Wells Fargo