Information Risk and the Evolution of the Security Rating Industry[1]

Igor Macura and Eric Johnson
Center for Digital Strategies
Tuck School of Business at Dartmouth

March 5, 2009

Abstract

Measuring Information risk within an enterprise has proved to be challenging. While there are obvious analogies to other risk rating activities, like financial credit risk, there are important differences. We present an analysis of approaches to evaluate information risk, with particular emphasis on the development of market incentives to drive wide-spread adoption. Examining information risk through the lens of the debt market rating industry, we consider the possibility of market-driven mechanisms to facilitate wide-spread information risk rating.

Introduction

Risk is part of every business decision. Many risks can be quantified, priced, and thus effectively management through financial instruments and portfolio management. Evaluating and rating the information security risk posed internally or by a business partner has proved to be a more significant challenge. Many initiatives are underway to develop a common reference for characterizing and pricing cyber security risk that is actionable in the marketplace.

In this paper, we examine different approaches for evaluating and measuring cyber risk. In particular we consider the possible marketplace development of external rating agencies. This is done via a comparison with the credit rating industry, one that has been prosperous for almost a century. Credit rating was chosen as a concept with the same underlying idea – that of bridging asymmetric information for a fraction of the cost of obtaining information. It is also probable that the long existence of the credit rating industry testifies on success factors, potentially applicable to the information security rating industry.

[1] This research was supported through the Institute for Information Infrastructure Protection (I3P) under awards 60NANB6D6130 from the U.S. Department of Commerce. The statements, findings, conclusions, and recommendations are those of the authors and do not necessarily reflect the views of the National Institute of Standards and Technology (NIST), the I3P, or Dartmouth College.

The paper is laid out as follows: section 1 offers a historical overview of the credit rating industry, a breakdown of the competition, and the rating process is described; section 2 introduces the notion of information security and some of the concepts created in attempt to systematically address information security; section 3 contains a comparison between investing in debt and outsourcing a service; section 4 concludes the paper.

1. The Credit Rating Industry

A credit rating is an opinion of the credit quality of individual obligations (such as a debt security) or of an issuer's general creditworthiness[2]. The specialized companies that issue the ratings are commonly referred to as credit rating agencies (CRAs).

Industry History

The credit rating industry was established in 1909, when John Moody published a book titled *Moody's Analyses of Railroad Investments*[3].

The *Analyses* were a step forward from Moody's first publication, *Moody's Manual of Industrial and Miscellaneous Securities*. Like a few other publications of the time, the *Manual* was a source of financial statistics, but without any judgment on the securities. As Moody's Manual Co. went bankrupt in 1907, John Moody came up with a plan to leverage his experience as a Wall Street analyst and not only publish raw data on securities, but also classify the securities in quality groups, a practice used in the then large investment companies. He used a simple mercantile rating scale to do this.

The *Analyses* contained data and ratings for more than 250 railroad bonds[4]. The volume proved a success - the whole circulation was sold within three months of the publication date.

John Moody said: "While (the book) raised a storm of opposition, not to mention ridicule from some quarters, it took hold with dealers and investment houses."[5]

The ratings coverage then expanded to industrial companies, utilities, and municipalities. By 1924, Moody's Investors Service issued ratings for nearly the entire US bond market.

---

[2] Moody's Ratings System, http://www.moodys.com/moodys/cust/research/mdcdocs/24/2005700000433096.pdf
[3] Moody's History, http://www.moodys.com/moodys/cust/AboutMoodys/AboutMoodys.aspx?topic=history
[4] Partnoy, F: *The Siskel And Ebert Of Financial Markets?: Two Thumbs Down For The Credit Rating Agencies*, Washington University Law Quarterly, Vol. 77:619, 1999, p. 638
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=167412
[5] As quoted in Partnoy, F: *supra*., p. 638

In 1931, the Office of the Comptroller of the Currency, the federal bank regulator, required of the banks to use current market prices for all the bonds on their balance sheet rated below "investment grade". This was the first case of a formal regulatory endorsement of debt ratings.

In 1936, the OCC went further and restricted banks from buying bonds below "investment grade".

In the following decades, dozens of regulations included references to ratings, increasing the influence of CRAs.

Until 1969, CRAs derived their revenue exclusively from selling the ratings publications to the investment public. This was the "investor-pay" business model. In 1969, S&P started charging the issuers of municipal bonds for rating the bonds[6].

The proliferation of photo-copiers in the 1970s made appropriating the value from ratings a difficult task for the CRAs, due to a growing number of free-riders. This is what made CRAs reconsider their business model, but it would be unfair to say that photo-copiers alone caused the switch from investor-pay to issuer-pay.

A high-profile bankruptcy of Penn Central, a railway company, shook the confidence of investors in corporate debt and issuers rushed to do anything they could to reassure the investors of their creditworthiness[7]. Obtaining (good) credit ratings seemed a good idea, and thus the investors were willing to pay to be rated.

In 1975, SEC designated Moody's Investors Service, Inc. (Moody's), Standard & Poor's Division of the McGraw-Hill Companies, Inc. (S&P), and Fitch, Inc. (Fitch) as Nationally Recognized Statistical Rating Organizations (NRSROs). A number of SEC regulations included (and still include) provisions related to NRSROs, but which organizations these were remained unclear and disputable for decades. It is a privileged status: certain investors are only allowed to purchase securities rated (adequately) by an NRSRO[8]. For instance, Rule 2a-7 of the Investment Company Act of 1940 restricts the investment options of money market funds to debt rated "AA" or higher by an NRSRO[9]. This creates an immense competitive advantage for NRSROs over the other CRAs.

---

[6] A History of Standard & Poor's, http://www2.standardandpoors.com/spf/html/media/SP_TimeLine_2006.html
[7] Cantor, R. and F. Packer: *The Credit Rating Industry*, "Quarterly Review", Summer/Fall 1994, Vol. 19, Issue 2
[8] *Downgraded*. "The Economist", 00130613, 7/15/2006, Vol. 380, Issue 8486
[9] Ackerman, A: *SEC Votes to Remove NRSRO from 38 Rules,* "The Bond Buyer" http://www.bondbuyer.com/article.html?id=20080625YA9RHPDA

After receiving the NRSRO designation, the three CRAs could take full advantage of the new business model, by charging investors for providing them with ratings they needed to sell their securities successfully. Most of the other CRAs, however, still use the "investor-pay" model[10].

A combination of SEC's reluctance to issue more NRSRO designations and industry consolidation - four NRSROs merged with Fitch - produced a lasting oligopoly. Until 2003, there were only three NRSROs. In a series of moves aimed at promoting competition, SEC awarded several CRAs the NRSRO designation. As of September 2008, there were ten NRSROs[11]:

Nationally Recognized Statistical Rating Organizations
Realpoint LLC
LACE Financial Corp.
A. M. Best Company, Inc.
DBRS Ltd.
Egan-Jones Rating Company
Fitch, Inc.
Japan Credit Rating Agency, Ltd.
Moody's Investors Service, Inc.
Rating and Investment Information, Inc.
Standard & Poor's Ratings Services

Exhibit 1: Nationally Recognized Statistical Organizations

As a further step in boosting competition in the industry, the SEC decided in 2008 to remove references to NRSROs from its legislation[12].

Industry Participants

In this section, we describe the three main competitors - S&P, Moody's, and Fitch - whose combined market share is 95%[13].

Standard & Poor's

S&P was created in 1941, when Standard Statistics Inc. and Poor's Publishing Co. merged. Poor's Publishing was the successor of a company founded in 1868 that published the *Manual*

[10] Basel Committee On Banking Supervision, *Credit Ratings and Complimentary Sources of Credit Quality Information*, Working Papers No. 3, Basel, 2000, p. 3 http://www.bis.org/publ/bcbs_wp3.pdf?noframes=1
[11] Nationally Recognized Statistical Rating Organizations, http://www.sec.gov/divisions/marketreg/ratingagency.htm
[12] Ackerman, A: *supra*
[13] Whitehead, J. M. and H. S. Mathis: *Finding a Way Out of the Rating Agency Morass,* p. 6 http://www.house.gov/apps/list/hearing/financialsvcs_dem/htmathis092707.pdf

of the Railroads of the United States, an annual publication with information for railroad investors. The Standard Statistics Bureau, the predecessor of Standard Statistics Inc. was established in 1906 and published a manual on industrial companies that was frequently updated with corporate news. The two companies had published ratings since 1922 (Poor's Publishing) and 1923 (Standard Statistics). Standard Statistics also published market indices since 1923[14].

S&P became publicly traded in 1962. The company was acquired by McGraw-Hill Companies in 1966 and has operated as a division of McGraw-Hill ever since.

The division consists of two groups: Credit Market Services and Investment Services[15].

The Credit Market Services group produces credit ratings and risk evaluations. This group earned $2.26 billion in revenue in 2007, or 74% of S&P's total revenue.

The Investment Services group produces: financial data, investment research, and market indices. It sells products such as Capital IQ, and charges fees to exchange-traded funds (ETFs) linked to S&P indices, as well as to users of derivatives based on these indices. Some of the best-known indices include: S&P 500, S&P Europe 350, and S&P Global 1200.

S&P's 2007 revenue was $3.05 billion, and the operating profit $1.36 billion, implying a 45% operating margin. The division's revenues grew at a compounded annual growth rate of 14% in the period 2002-2007[16] and represented 45% of its parent company's revenue.

In 2007 S&P earned over 40% of its revenue abroad and had a 40% share in the US ratings market[17].

Moody's Corporation

Moody's Corporation was a successor of a company founded in 1914 by John Moody. This was John Moody's second attempt at running a business, as the first company he founded, Moody's Manual Co, was sold in 1907 due to financial difficulties, and was later merged into Poor's Publishing Co[1819].

---

[14] A History of Standard & Poor's, http://www2.standardandpoors.com/spf/html/media/SP_TimeLine_2006.html
[15] McGraw-Hill Companies 2007 Annual Report, http://www.mcgraw-hill.com/about/annual_report/ar_2007.pdf
[16] *Ibid*.
[17] Whitehead, J. M. and H. S. Mathis: *supra*, p. 6
[18] Moody's History, http://www.moodys.com/moodys/cust/AboutMoodys/AboutMoodys.aspx?topic=history
[19] A History of Standard & Poor's, http://www2.standardandpoors.com/spf/html/media/SP_TimeLine_2006.html

In 2008, Moody's represented the only stand-alone credit rating agency among the big three. It was listed in 2000, after spinning off from Dun & Bradstreet, a business intelligence provider. Dun & Bradstreet had acquired Moody's in 1962[20].

Moody's Corporation comprised two segments: Moody's Investors Service and Moody's Analytics.

Moody's Investors Service issued multiple types of credit ratings, such as those for corporate and governmental debt, and structured finance products.

Moody's Analytics performed and published credit research, industry studies and special opinions. In addition, it sold credit risk assessment products and services, such as analytical tools for credit portfolio management and credit processing software.

In 2007, Moody's Investors Service made $1.84 billion in revenue, and had an operating profit of $1 billion, which translates into an operating margin of 54%. Structured finance ratings revenue was $0.89 billion, or a half of the segment's total third-party revenue[21] and 39% of the company's total revenue.

The company's total revenue in 2007 was $2.26 billion, with an operating profit of $1.13 billion, and an operating margin of 50%. The company earned 40% of its revenue internationally. Moody's held 39% of the US ratings market[22].

Fitch Ratings

The history of Fitch Ratings began with the establishment of Fitch Publishing Company, a publisher of financial statistics, in 1913.

The company remained independent until 1997, when it was acquired by Fimalac, a French-based financial information provider. Fimalac had already owned IBCA, another credit rating agency, and merged the two into Fitch IBCA. The company then acquired two more credit rating agencies, Duff & Phelps and Thomson Bankwatch (both in 2000)[23].

[20] The History of D&B, http://www.dnb.com/us/about/company_story/dnbhistory.html
[21] The third-party revenue for Moody's Investors Service was $1.78b - somewhat lower than the segment's total revenue, as a consequence of an inter-segment royalty.
[22] Whitehead, J. M. and H. S. Mathis: *supra*, p. 6
[23] The History of Fitch Ratings, http://www.fitchratings.com/jsp/corporate/AboutFitch.faces?context=1&detail=3

Fitch Ratings and Algorithmics had 2007 revenue of $0.93 billion, representing 85% of Fimalac's total revenue[24], and an operating profit of $0.29 billion, or a 31% operating margin in 2007.

Algorithmics is a producer of enterprise risk management solutions, such as credit risk, capital management, and operational risk products.

Fimalac earned roughly a half of its revenue in the US and Fitch Ratings had a 16% share in the US ratings market[25] in 2007.

The Rating Process[26]

The rating process is typically[27] initiated by an issuer requesting a rating. The issuer then submits annual reports for the past five years and several most recent interim reports, as well as descriptions of businesses and products to the CRA. These documents are used for initial analysis. The CRA analysts then meet the issuer management to discuss: industry environment, operating results, financial and accounting policies, financial projections and financing alternatives. The lead analyst then presents the conclusions to the rating committee, a body of 5 to 7 voting members, and the committee votes on the rating. The issuer is then notified on the rating and given a short period to protest the rating by presenting more information. In case there is an appeal, the rating committee meets again and there is a new vote on the rating. The rating is then published. This process is shown in exhibit 2.

[24] Data for year ended September 30, 2007, translated into USD values using the EUR/USD exchange rate as of September 30, 2007. The original data can be retrieved from: http://www.prline.com/rootMRI/3794/docsMRI/RA-2007-GB.pdf

[25] Whitehead, J. M. and H. S. Mathis: *supra*, p. 6

[26] The discussion builds heavily on Standard & Poor's: *Corporate Ratings Criteria,* http://www2.standardandpoors.com/spf/pdf/fixedincome/corprate_criteria_2008.pdf

[27] Unsolicited ratings are also issued, but present a small fraction of the total ratings. For more on this, see: *Who rates the raters?* "The Economist", 00130613, 3/26/2005, Vol. 374, Issue 8419

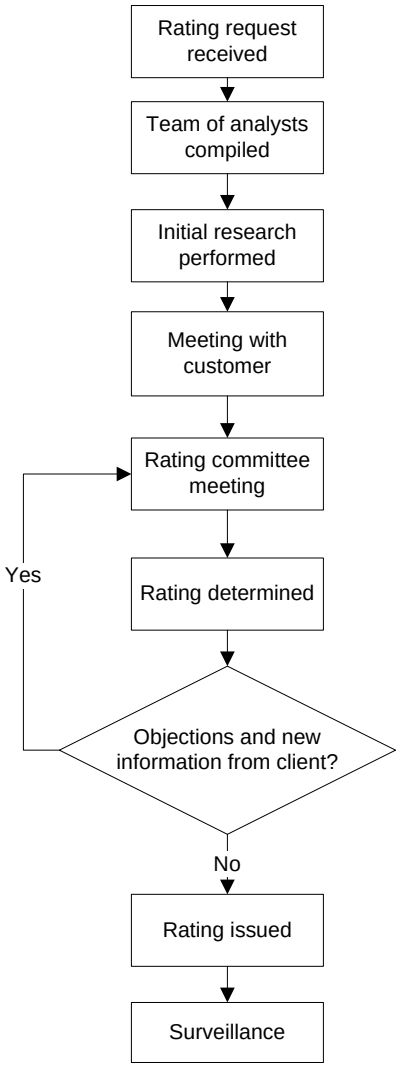

Exhibit 2: The rating process at Standard & Poor's[28]

The criterion of the rating committee typically depends on the type of the issuer and the nature of the rating. The rating methodology is different for corporations, financial institutions, governments, and local authorities.

The rating can be an issuer rating, where the issuer's overall creditworthiness is assessed, or an issue rating, which pertains to a specific securities issue.

[28] For more, see Crouhy, M. and D. Galai, R. Mark: *Prototype risk rating system*, "Journal of Banking & Finance", Volume 25, Issue 1, January 2001, p. 53

In order to explain the rationale for assigning a rating, we will use the example of corporations. The creditworthiness of a corporation or an individual issue of corporate debt is a function of 1) business risk and 2) financial risk.

1) Business risk profile reflects the challenges the business environment poses to a company. The components of business risk are: country risk, industry factors, competitive position, and relative profitability.
   Country risk is measured to some extent by sovereign ratings, but these ratings do not fully capture the intensity of government impact on the business environment.
   Industry factors are such things as the industry life-cycle phase, competition intensity, industry concentration level, key competitive factors etc.
   Competitive position assessment is based on considerations of the company's size, level of diversification, availability of critical resources etc.
   Profitability is critical for debt-repayment. However, profitability must also be benchmarked against the comparable companies for potential signs of problems.
   All these considerations lead to a conclusion about the issuer's business risk profile.
2) Financial risk assessment follows the evaluation of the issuer's business risk. The components of financial risk are: financial policy, accounting, cash flow adequacy, capital structure, and liquidity/short-term issues.
   Financial policy: A clearly defined, detailed, and reasonable financial policy reflects the management's awareness of the financial issues it has to deal with and is a sign of a higher potential of handling financial difficulties.
   Accounting: there is a risk arising from the accounting characteristics of the issuer, i.e. the frameworks and methods used in compiling financial statements, the degree of disclosure, and the cross-company comparability.
   Cash flow adequacy: A cash flow analysis needs to supplement the profitability analysis because of significant differences between the income statement and cash flow statement. As the debt obligations need to be settled in cash, the income statement is not a reliable source of information on debt-repayment ability of the issuer.
   Liquidity/short-term issues: In case there are particular problems that were not addressed in other sections, they are discussed here. Examples are pending lawsuits and other contingencies.
   Once the issuer's financial risk profile is assessed, the rating can be determined as a function of two risk profiles – for instance, a high business risk profile combined with a low financial risk profile will result in a moderate rating.

It is worth noting that many of the risk factors cannot be measured. This is especially true of the business risk factors. What is done instead of measurement is a series of qualitative considerations. Exhibit 3 offers an example of this for industry risk. Competition is denoted as

having a high impact on credit risk in all ten industries, yet it does not mean that competition is equally unfavorable in each of the industries.

While cash flow analysis and some other elements are strictly quantitative, the rating process as a whole is not a string of calculations, but a detailed discussion and is therefore subject to judgment of the members of the rating committee.

Table 3 Key Industry Characteristics And Drivers Of Credit Risk

Credit risk impact: High (H); Medium (M); Low (L)

Risk factor	Cyclicality	Competition	Capital intensity	Technology risk	Regulatory/ government	Energy sensitivity
Industry	H	H	H	L	M/H	H
Airlines (U.S.)	H	H	H	M	M	H
Autos*	H	H	H	M	M	M
Auto suppliers*	H	H	M	H	L	L/M
High technology*	H	H	H	M	M/H	H
Mining*	H	H	H	L	M	L
Chemicals (bulk)*	H	H	H	L	M	H
Hotels*	H	H	H	L	L	M
Shipping*	H	H	H	L	L	M
Competitive power*	H	H	M	L	H	H
Telecoms (Europe)	M	H	H	H	H	L

*Global.

Exhibit 3: A breakdown of risk factors for certain industries[29]

The long-term debt rating scales of the three biggest CRAs are shown in Exhibit 4. The ratings are sorted from highest to lowest. Debt rated from "AAA" ("Aaa") to "BBB" ("Baa") is considered investment grade, whereas debt rated lower is considered speculative grade. Each of the ratings can be added a modifier to signal that the rated debt is in a higher or lower end of its generic category. These modifiers are "+" and "-" for the S&P/Fitch scale, and "1", "2", and "3" for the Moody scale. A "+" ("1") means that debt is in the higher end of its generic category, whereas a "-" ("3") means that it is in the lower end. For the medium area of a generic category, S&P and Fitch do not use a modifier, whereas Moody's uses "2".

Even though these scales are technically very similar (or even identical, for S&P and Fitch), that is not to say that the meanings of the ratings are quite compatible. There are significant

[29] Standard & Poor's *Corporate Ratings Criteria,* http://www2.standardandpoors.com/spf/pdf/fixedincome/corprate_criteria_2008.pdf p. 27

differences in ratings assigned by S&P and Moody's in cases when both CRAs have rated debt issues[30].

Standard & Poor's/Fitch	Moody's
AAA	Aaa
AA	Aa
A	A
BBB	Baa
BB	Ba
B	B
CCC	Caa
CC	Ca
C	C

Exhibit 4: Long-term debt rating scales of Standard & Poor's, Moody's and Fitch[31]

Conjectures on Success Factors of Credit Rating

If the first customers of *Moody's Analyses* were "dealers and investment houses", as John Moody claims, several key success factors can be identified:

1. Simplicity: Moody's scale was new to the investment professional, but was easily comprehensible;
2. Scope: all the railroad debt securities were rated, and everyone interested in investing in these knew that the volume would help;
3. Comparability: the above two factors enabled quick and effective comparisons across securities;
4. Accuracy: while it may be hard to believe that Moody's ratings were more accurate than the opinions of the investment professional, but they were good enough in that the time savings they provided more than compensated for the possible loss of decision quality.

The success factors changed dramatically with the government regulation. While CRAs have maintained the abovementioned features, the NRSRO status was until recently their most important trait, because it enables the CRAs to decide on the cost of financing of public companies by assigning ratings to them.

---

[30] See, for example: Cantor, R. and Packer, F: *Sovereign credit ratings*, "Current Issues in Economics & Finance", 19362374, Jun95, Vol. 1, Issue 3

[31] Sources: Standard & Poor's Ratings Definitions http://www2.standardandpoors.com/portal/site/sp/en/us/page.article/2,1,1,4,1204838038012.html#ID217, Moody's Long-Term Rating Definitions http://www.moodys.com/moodys/cust/AboutMoodys/AboutMoodys.aspx?topic=rdef&subtopic=moodys%20credit%20ratings&title=Long+Term+Obligation+Ratings.htm

2. Information Security

The advances in information and communication technology of the 1990s and 2000s have significantly broadened the scope of interaction between organizations and individuals. While this development means new business opportunities for companies, such as process acceleration, outsourcing, telecommuting, it also bears with it increased risks for the IT infrastructure of organizations. These risks manifest themselves through: hacker attacks, spyware proliferation, various types of data theft, virus infections, etc. These risks can cause costs associated with reputational damage, production delays, lawsuits etc. A number of initiatives emerged in an attempt to help mitigate these risks, resulting in frameworks for maintaining and improving information security and specialized commercial services. We will discuss several of these initiatives.

ISO/IEC 27002:2005

ISO/IEC 27002:2005 is a joint publication of the International Organization for Standardization and the International Electrotechnical Commission. The Standard is a set of general guidelines on information security and is intended as a starting point for building organization-specific guidelines for information security[32]. It views the implementation of information security as a managerial process that needs to be in line with the business goals of the organization.

The Standard defines 39 main security categories and groups them into 11 clauses[33]:

1. Security Policy;
2. Organizing Information Security;
3. Asset Management;
4. Human Resources Security;
5. Physical and Environmental Security;
6. Communications and Operations Management;
7. Access Control;
8. Information Systems Acquisition, Development and Maintenance;
9. Information Security Incident Management;
10. Business Continuity Management;
11. Compliance.

Each main security category contains a control objective and controls to use in order to achieve this objective. For every control, implementation guidance offers more specific information on

[32] ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management, Second edition, p. xi
[33] *Ibid*, p. 4

how to implement it. The control descriptions also contain other information, such as references to other standards and other important notes.

The organizations applying the Standard are advised to assess the importance of individual controls against the risks they are facing, as some controls will prove more relevant than others[34]. Certain organizations will require some controls that are not included in the Standard. Moreover, the Standard does not deal with methodological issues of information security measurement. Therefore, applying ISO/IEC 27002 is a signal of the organizational awareness of the importance of information security, but not a conclusive proof that the organization successfully deals with information security issues.

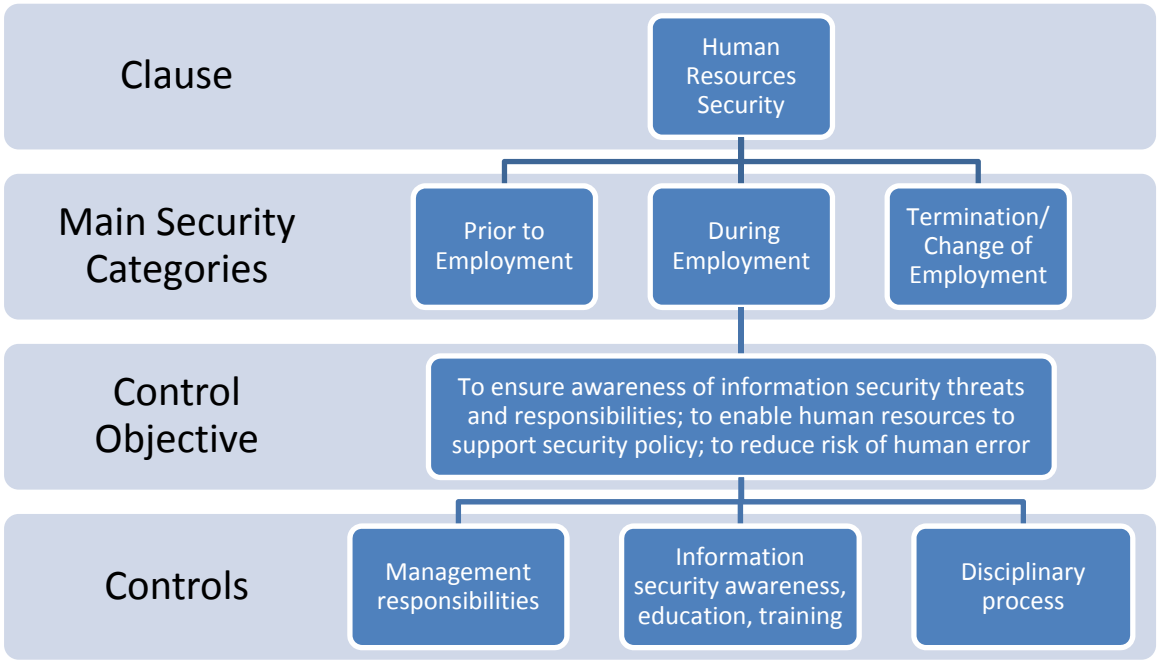

Exhibit 5: An illustration of the ISO 27002 structure[35]

[34] *Ibid*, p. x
[35] The diagram was drawn using information from *Ibid*, p. 23-27

CERT® Resiliency Engineering Framework[36]

The CERT® REF is a manual for improving organizational capabilities from a security and business continuity standpoint. It is based on the idea that security is a company-wide concern, rather than a strictly technical concern. The Framework proposes a process improvement approach and defines the resiliency engineering process as consisting of 26 elements[37], called capability areas. A capability area is a set of practices performed towards meeting the goals of a process. The capability areas are organized in four categories[38]:

- Enterprise management
- Engineering
- Operations
- Process management

The enterprise management capability areas are those built in the processes that support the resiliency engineering process.

The engineering capability areas are related to establishing and increasing the resiliency of the organizational assets, business processes, and services. The operations capability areas are focused on managing the operational resiliency of assets and services. Finally, the process management capability areas encompass the processes aimed at measuring, managing, and improving the resiliency engineering process. Exhibit 6 shows the capability areas by these four categories[39].

Each capability area is described by the following elements[40]: purpose statement, introductory notes, related capability areas, baseline goals and specific practices, typical process artifacts, subpractices, and elaborated common goals and practices.

The purpose statement broadly define the goals of the capability area, while the baseline goals and specific practices explain the partial goals and provide more detail on how to achieve them. The introductory notes explain the importance of the capability area and introduce the special

---

[36] The discussion is based on version 0.95 of the document, a version released for the purpose of enabling reviews and collecting comments: CERT® Resiliency Engineering Framework, version 0.95 http://www.sei.cmu.edu/community/resiliency-engineering/REFramework.zip

[37] Version 0.95 contains details on only 21 capability areas, but additional five areas are announced to be elaborated in future versions. Ibid, p. 4

[38] *Ibid*., p. 13

[39] By this diagram, we do not intend to suggest that the Framework recommends a "silo" approach to resiliency.

[40] *Ibid*., p. 10

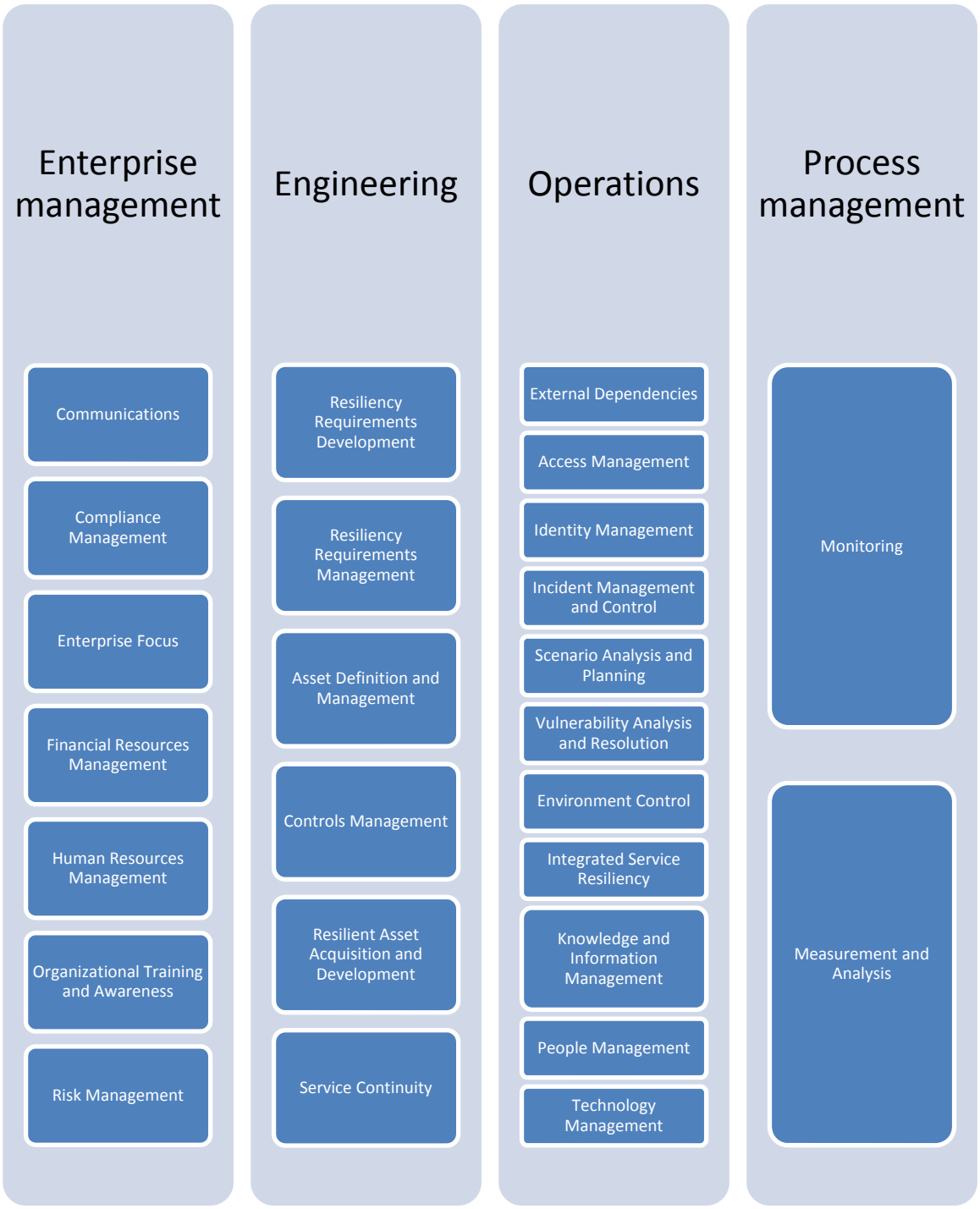

Exhibit 6: CERT® REF Capability areas by category

terminology. The related capability areas emphasize compatibility between certain areas – a matter to consider when contemplating the improvement of a capability area. Typical process artifacts are examples of suitable informative elements for specific practices. Subpractices are hands-on recommendations on how to perform specific practices and achieve common goals. Elaborated common goals and practices contain examples and explanations on how to achieve

goals and perform practices for every capability level. A sample of the Framework's hierarchy from capability area down is given in Exhibit 7.

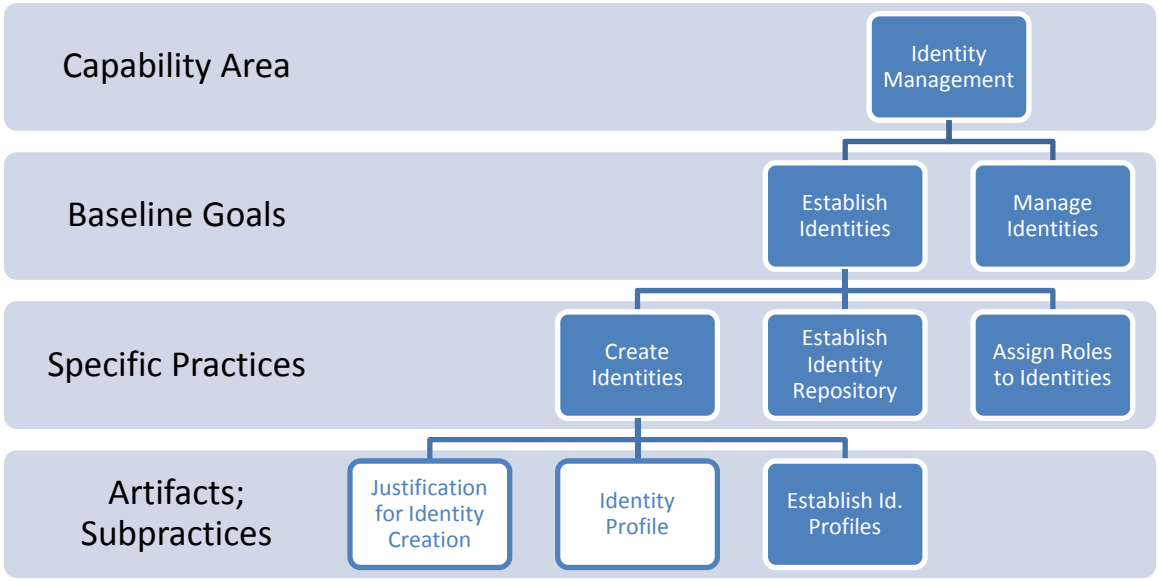

Exhibit 7: An illustration of the CERT® REF hierarchy[41]

The Framework defines five capability levels, marked with a number and a brief qualitative title. The numbers range from 0 to 4, where Level 0 (Incomplete Capability) is the lowest, and Level 4 (Continuously Improved Capability) the highest. The Framework does offer a description for each of the capability levels, but the Resiliency Engineering Framework team is still developing comprehensive guidance for organizational self-evaluation[42]. Once this is in place, organizations using REF will be able to make estimates of their capability levels for each capability area, and set improvement targets.

BITS FISAP

BITS is a branch of the Financial Services Roundtable, a consortium of 100 of the biggest financial institutions in the US. BITS was created to help the electronic financial service and e-commerce efforts of financial institutions[43].

The BITS Financial Institutions Shared Assessments Program (FISAP) was designed in the wake of a growing reliance on outsourcing among financial institutions. It was envisioned as a tool

[41] The diagram was drawn using information in *Ibid.*, p. 174-186
[42] *Ibid.*, p. 9
[43] About BITS, http://www.bitsinfo.org/about.html

that will make collection of vendor security information a more efficient and more uniform process, and will result in raising the information security standards in the vendor universe[44].

FISAP comprises two components: Agreed upon Procedures (AUP) and Standardized Information Gathering Questionnaire (SIG).

AUP contains instructions for assessment firms (such as audit companies) on how to inspect elements of a vendor's information security system. The control areas are the same as clauses in ISO 27002, with one additional control area – Risk Management. The document is organized as a set of checklists, and, since it was designed with the financial service industries in mind, it is more specific than ISO 27002.

AUP is applied in the following way: a vendor agrees with an assessment firm on the scope of the tests, i.e. which control areas will be tested, the assessment firm performs the test following the AUP guidelines, and then the assessment firm issues a report of findings. The content of the report is objective and does not encompass the opinion of the assessment firm.[45]

The vendor uses the report to improve its information security system, because the report points out its weaknesses.

The (potential) users of the vendor's services can obtain the report from the vendor and compare them to their risk appetites and/or to other vendors' reports. The latter comparison is possible due to the standardized format of the tests performed.

SIG is a self-evaluation tool for vendors organized as a set of spreadsheets with yes/no questions. The questions are grouped in control areas identical to those laid out in the AUP document. SIG requires less of a time and resource commitment than AUP (especially its condensed component, SIG Lite)[46], but is also less reliable, given that the questionnaire is filled by the vendor, and that there is no attestation by a third party.

Moody's Vendor Information Risk Rating[47]

Moody's Risk Services Group combines Moody's credit rating expertise with the standardization efforts the financial institutions are investing in making the most of outsourcing. It launched a Vendor Information Risk service, ideally positioned as a cheaper and a more efficient alternative to BITS FISAP.

---

[44] BITS Shared Assessments Program, Agreed Upon Procedures Version 3.0, p. 5
[45] *Ibid.*, p. 8
[46] BITS, BSI Management Systems, An Integrated Approach: ISO 27001 and BITS Shared Assessments Program, p. 7-8, http://www.bitsinfo.org/FISAP/Forms/ISOWP2008.pdf
[47] For a detailed discussion of this service, please see Appendix.

The service was designed to address two key drawbacks of BITS FISAP: 1) time and resources of the financial institutions and their vendors. 2) lack of easy summarization. The output of an evaluation using the BITS Agreed upon Procedures discussed above takes the form a report on findings, but does not contain a single "grade" that would summarize the vendor's information security level. This makes reviewing the reports time-consuming, and comparing them across vendors difficult, if not equivocal (for instance, vendor "A" has a more compelling information security policy, but vendor "B" has a better asset management record – which one is more reliable?).

Moody's assigns two types of ratings to vendors – overall security quality ratings and inherent risk ratings (inherent risk is the risk incorporated in the vendor's business environment).

3. A Comparison of Debt Rating and Information Security Rating

At a first glance, there are numerous similarities between debt rating and information security rating. Debt ratings are an important input for investors making decisions on purchasing, selling or holding debt securities. They are vital for companies issuing debt as a proof of the value of the debt and a catalyst for obtaining financing.

It is possible to view outsourcing as a special type of investing. The customers invest by making contracts with vendors, who in turn commit to delivering products or services of a certain level of quality. This is comparable to the interest and principal payments on debt securities. As in the case of debt, the clients ("investors") know significantly less about what the vendors ("issuers") are offering than the vendors themselves. In other words, there is asymmetric information that could lead to suboptimal decisions on the part of the clients.

The Differences between Investing in Debt and Outsourcing

Payoff: The yields on the riskiest bonds reach are on average 5.42%[48] above the yields on treasury bonds, which in turn are slightly higher than the inflation rate. The savings from outsourcing range from 12% to 17% of the projected costs[49] and outsourcing can produce a number of benefits difficult to quantify, such as: quality improvement, increased reliability, cost standardization, redeployment of staff to more productive tasks.

On the other hand, in the most extreme case of bad decision-making, a bond investor loses the entire amount invested in a bond whose issuer defaulted, while a client in an outsourcing deal can lose much more than what the contract is worth. This is because the client may be forced

[48] Rattner, S: *The Coming Credit Meltdown,* "The Wall Street Journal", June 18, 2007

[49] Roehrig, P: *Outsourcing Clients Can Expect 12% To 17% Savings*
http://www.forrester.com/Research/PDF/0,5110,43255,00.pdf

to bear the damage due to a loss or abuse of confidential information on the part of the vendor.

We can conjecture that the variance in the profitability of outsourcing contracts is much higher than that of the bonds, and this has two implications: 1. some companies are reluctant to enter outsourcing contracts because they are not willing to accept the high risk that they carry and 2. improvements in decision-making in outsourcing bring higher marginal benefits than those in bond investing.

Diversification: A bond investor can reduce the idiosyncratic risk in its bond portfolio by diversifying, i.e. purchasing bonds of different companies in different industries instead of just putting all its money in bonds of a single company. Thus, if one of the companies in the portfolio fails, the investor will only bear a fraction of the cost it would incur if the whole portfolio consisted of bonds of the bankrupt company. The transaction costs of doing this are negligible, and there is no need to sacrifice any of the yield, which means that diversification is virtually free.

Many companies have a large number of vendors, but this does not indicate diversification effort as much as the fact that there are many different services and/or geographic areas in which the companies are outsourcing. There are at least two reasons why diversification makes far less sense in outsourcing: 1. the contractual costs are significant and 2. some risks may be diluted, but some may be increased by diversification.

One of the foremost motives for outsourcing are savings, and spending large sums of money on negotiating outsourcing contracts with multiple vendors can bury the hope of achieving savings before outsourcing even begins.

If a vendor provides a vital input for the client, having two or more vendors may be a good idea in the interest of business continuity. However, having multiple vendors for the same service eats into the economies of scale and standardization and may also increase risks associated with bad publicity, lost revenues etc.

Liquidity: Once an investor is made aware of the difficulties an issuer is facing, it can sell its holding of the investor's bonds, typically at a small loss, and move its money into bonds of another issuer. It can also keep the holding, expecting the issuer to recover and deliver on its contractual obligations.

If a vendor is having difficulties, a client cannot walk away as freely. The costs of terminating an outsourcing contract consist of: a contract termination fee, the cost of looking for a replacement and costs associated with implementing an interim solution, such as reassigning

staff and/or suffering a lower quality service. Another option is for the client to work with the vendor to help it overcome the problems, but this comes at a high cost as well.

Alternative sources of information: In order to judge the likelihood of default of an issuer, an investor can choose from many sources of information: SEC filings, business news, market data, ratings etc. Indeed, studies indicate a small impact of a change in the rating of a bond, which implies that there is little new information contained in the new rating.

There is very little publicly available data on information security of individual companies. This type of information is highly sensitive and companies strive to keep a low profile, so as to minimize the risk of their weaknesses being exploited. Therefore, what little information is published is normally bad news about compromised data. The usual way of collecting vendor information is via a due diligence, a process that costs hours of work of highly trained staff and hours of the vendor's time.

Companies interested in outsourcing would almost certainly benefit from information security rating, regardless of whether they would use them as a replacement or as a supplement for a due diligence.

Organizational issues: A successful investment record results in benefits for the investor and for the individuals making the investment decisions. Successful outsourcing, though, can yield ambiguous consequences: while the company as a whole prospers, as well as the individuals responsible for outsourcing, some other staff may become redundant and laid off. The prospects of outsourcing can create resistance within a company and some companies may dismiss the very idea of outsourcing.

4. Conclusion

The pronounced risk of outsourcing makes the demand for outsourcing lower than it could be, but this also signals a great opportunity for market growth. If a rating company can offer reliable assistance in mitigating this risk, it can count on an extended period of high revenue growth.

While producing the information security ratings is costly compared to producing debt ratings, there is still plenty of room for healthy profits because the alternative information collection method is very expensive and may not even stand in the way of the ratings - a second opinion is desirable, not least because a client may be biased towards a certain outsourcing decision.

Like the early credit rating industry, information security rating business will be reputation-based. Few companies can claim to be known as reliable in assessing company information security. Audit firms are among these, but their involvement in the industry is questionable due

to the potential cannibalization effect, namely with the on-demand audits for a single client. Most other companies will have to start from zero credit and that could mean fierce competition.

Initially, the whole industry would benefit from high competition because it would gain momentum faster and its legitimacy would be established sooner. This would result in the inclusion of the hesitant companies in the customer base. Coexistence of multiple rating companies would last for years before market determines the companies with the best track record. Alternatively, a dominant company may emerge right from the start if one competitor decides to take a “big-bang” approach, covering a great number of vendors in a short time. The rating reports of others would then be perceived as exotic and of little value because few comparisons could be made.

A serious obstacle to the growth of the industry may be the fact that the ratings and the rating reports are confidential. This is not only because the market is then automatically narrowed down to the trustworthy companies, but also because obtaining the reports is more difficult and requires trilateral contacts – between the client, the rating company, and the rated vendor. Besides, anonymous shopping is disabled – another discouraging detail.

The idea of informational intermediation is clearly superior to the current solutions, which are costly, and suffer from redundancy, on the one hand, and a lack of resources, on the other. Whether the information security rating industry will be established is not the question; but rather how quickly, at what the level of competition, and with the emergence of which major players.

REFERENCES

Ackerman, A. (2008): *SEC Votes to Remove NRSRO from 38 Rules,* "The Bond Buyer" http://www.bondbuyer.com/article.html?id=20080625YA9RHPDA

Basel Committee on Banking Supervision (2000), *Credit Ratings and Complimentary Sources of Credit Quality Information*, Working Papers No. 3, Basel, http://www.bis.org/publ/bcbs_wp3.pdf?noframes=1

BITS (2008): *About BITS*, http://www.bitsinfo.org/about.html

BITS (2008): *BITS Shared Assessments Program, Agreed Upon Procedures Version 3.0*,

BITS (2008): *BSI Management Systems, An Integrated Approach: ISO 27001 and BITS Shared Assessments Program*, http://www.bitsinfo.org/FISAP/Forms/ISOWP2008.pdf

Cantor, R. and F. Packer (1994): *The Credit Rating Industry*, "Quarterly Review", Summer/Fall, Vol. 19, Issue 2

Cantor, R. and Packer, F (1995): *Sovereign credit ratings*, "Current Issues in Economics & Finance", 19362374, June, Vol. 1, Issue 3

Carnegie Mellon University's Computer Emergency Response Team (2008): *CERT® Resiliency Engineering Framework, version 0.95* http://www.sei.cmu.edu/community/resiliency-engineering/REFramework.zip

Crouhy, M. and D. Galai, R. Mark (2001): *Prototype risk rating system*, "Journal of Banking & Finance", Volume 25, Issue 1, January

Dunn & Bradstreet (2008): *The History of D&B*, http://www.dnb.com/us/about/company_story/dnbhistory.html

The Economist (2005): *Who rates the raters?*, 00130613, 3/26/2005, Vol. 374, Issue 8419

The Economist (2006): *Downgraded*, 00130613, 7/15/2006, Vol. 380, Issue 8486

Fimalac (2008): *Fimalac 2007 Annual report* http://www.prline.com/rootMRI/3794/docsMRI/RA-2007-GB.pdf

Fitch Ratings (2008): *The History of Fitch Ratings*, http://www.fitchratings.com/jsp/corporate/AboutFitch.faces?context=1&detail=3

International Organization for Standardization, International Electrotechnical Commission (2005): *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management*, Second edition, p. xi

McGraw-Hill Companies (2007): *McGraw-Hill Companies 2007 Annual Report*, http://www.mcgraw-hill.com/about/annual_report/ar_2007.pdf

Moody's (2005): *Moody's Ratings System,* http://www.moodys.com/moodys/cust/research/mdcdocs/24/2005700000433096.pdf

Moody's (2008): *Moody's Long-Term Rating Definitions,* http://www.moodys.com/moodys/cust/AboutMoodys/AboutMoodys.aspx?topic=rdef&subtopic=moodys%20credit%20ratings&title=Long+Term+Obligation+Ratings.htm

Moody's (2008): *Moody's History,* http://www.moodys.com/moodys/cust/AboutMoodys/AboutMoodys.aspx?topic=history

Partnoy, F (1999): *The Siskel And Ebert Of Financial Markets?: Two Thumbs Down For The Credit Rating Agencies*, Washington University Law Quarterly, Vol. 77:619, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=167412

Rattner, S (2007): *The Coming Credit Meltdown,* "The Wall Street Journal", June 18

Roehrig, P. (2007): *Outsourcing Clients Can Expect 12% To 17% Savings* http://www.forrester.com/Research/PDF/0,5110,43255,00.pdf

Securities and Exchange Commission (2008): *Nationally Recognized Statistical Rating Organizations*, http://www.sec.gov/divisions/marketreg/ratingagency.htm

Standard & Poor's (2006): *A History of Standard & Poor's,* http://www2.standardandpoors.com/spf/html/media/SP_TimeLine_2006.html

Standard & Poor's (2008): *Corporate Ratings Criteria,* http://www2.standardandpoors.com/spf/pdf/fixedincome/corprate_criteria_2008.pdf

Standard & Poor's (2008): *Standard & Poor's Ratings Definitions,* http://www2.standardandpoors.com/portal/site/sp/en/us/page.article/2,1,1,4,1204838038012.html#ID217,

Whitehead, J. M. and H. S. Mathis (2007): *Finding a Way Out of the Rating Agency Morass,* http://www.house.gov/apps/list/hearing/financialsvcs_dem/htmathis092707.pdf

APPENDIX

Moody's Risk Services VIR (Vendor Information Risk) Ratings

Strong Incentives for Paying Attention to Information Security

When a company is outsourcing a business process, the information security level of the vendor is one of the most important concerns. A loss of data due to inadequate data management on the part of the vendor typically causes a damage that far exceeds the benefits of outsourcing.

This is particularly true in the case of financial institutions, which handle highly sensitive data, the abuse of which can result in windfalls for the offenders. In such cases, financial institutions sustain costly blows: they must recover the immediate financial damage, but they also face bad publicity and, consequently, a loss of customers.

The stakes are higher for the vendors of financial institutions as well, because their exposure to information threats is proportionate to the value of the data they manage.

Moreover, financial institutions are concerned with information security because tend to rely heavily on outsourcing, and many of them have thousands of vendors. In addition, financial regulators put pressure both on the entities under their jurisdiction and on their vendors to make information security improvements.

Inefficiencies of Existing Verification Mechanisms

Traditionally, a financial institution wanting to verify the quality of a vendor's information security practices needs to run a due diligence, which comprises interviews and on-site visits. Notwithstanding the skillfulness of the teams performing the process, the number of vendors makes achieving anything close to regularity in the assessments an impossible task. Therefore, financial institutions choose to attend to the most critical vendors regularly, and visit the others when an opportunity shows, often in intervals longer than a year[50].

This situation poses three problems:

1. Lack of vendor information, which disables timely and appropriate reactions, leading to increased costs of outsourcing
2. Inability of the financial institutions to use their IT staff for other tasks, such as application development
3. Higher costs for vendors, which need to maintain staff for client assessments.

[50] In an interview held on August 14, 2008, Phil Venables of Goldman Sachs said that his company visits between 300 and 400 of more than 2000 vendors it has.

Formation of Moody's VIR Ratings

BITS FISAP was created with the goal of making vendor assessment an easier and less time-consuming task. However, the program had to accommodate requests from a number of diverse financial institutions, which made the SIG questionnaire difficult to fill and analyze, and the program has proved a disappointment for some financial institutions.

Thus in May 2007 Goldman Sachs, then an investment bank, contacted Moody's, a major credit rating agency, and suggested starting a new rating service – one dealing with vendor information risk[51].

Moody's hired Ed Leppert to run the service, as a Vice President. Leppert managed security assessment at Symantec, a security software giant, and @stake, a security consulting company acquired by Symantec in 2004. Leppert then hired John Nye, whom he worked with at @stake.

While at @stake, Leppert and Nye performed information security assessments, as a foot in the door for selling @stake's product. They saw tremendous value in the assessments, but realized @stake could not charge for this service due to its conflict of interests: the company developed software and used the assessments as a sales driver.

The idea of having Moody's perform the assessments made sense for Leppert and Nye, because expressing opinions is what Moody's core business is all about.

In creating its methodology, which is still a work in progress, Moody's leveraged an "advisory council" consisting of around a dozen financial institutions, including the abovementioned Goldman Sachs, Morgan Stanley, and Citigroup. These companies shared their own vendor assessment methodologies with Moody's. Moody's now claims that its assessments cover roughly 90% of the areas of interest of any of the financial institutions[52].

Rating System

Moody's assigns two types of ratings to vendors – overall security quality ratings and inherent risk ratings (inherent risk is the risk incorporated in the vendor's business environment).

For overall security quality ratings, the following scale is used:

VIR 5: Excellent

VIR 4: Strong

[51] Royal Hansen of Goldman Sachs and John Nye of Moody's on August 11, 2008 and by Ed Leppert of Moody's and Phil Venables of Goldman Sachs on August 14, 2008.

[52] The percentage was used by Nye and Leppert in the interviews on August 11 and 14, respectively.

VIR 3: Good

VIR 2: Needs Improvement

VIR 1: Poor.

The ratings can accompanied by a modifier, "+" or "-".

Inherent risk can be rated as low, medium, or high. The inherent risk ratings are obtained by analyzing the threat levels for 25 threat categories. Threat categories include: hacking, phishing, data loss etc.

The overall security quality ratings are based on the estimates of 11 "security fundamentals" – categories that strongly correspond to the ISO clauses, with the exception of Privacy, which Moody's also evaluates[53].

Each of the security fundamentals is rated using the VIR scale. The overall rating is a summary of these ratings, and it reflects not the absolute level of information security, but it takes into account the inherent risk the vendor is facing. Hypothetically, this means that, if vendor "C" and vendor "D" have identical information security controls, but "C" operates in a riskier business than "D", then "D" will get a better VIR rating.

An illustration of the rating process is shown in exhibit A1.

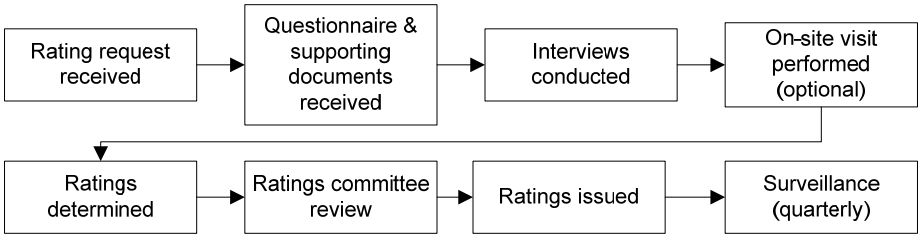

Exhibit A1: The rating process for Moody's information security ratings[54]

Once an assessment is complete, Moody's presents a report which summarizes the findings. An interested party that wants to purchase a report needs to obtain permission from the evaluated company. This practice serves the purpose of keeping sensitive information away from the eyes of competition or anyone else who wants to exploit the discovered vulnerabilities.

[53] Moody's: Vendor Risk Assessment: Moody's Vendor Risk Rating Service & Avior Solution Overview, webinar http://www.moodysriskservices.com/news_events/media/webinar_avior_moodys.wmv

[54] Based upon the information in id.

Business Model

Moody's charges the vendors $23,000 for the assessments and $10,000 per year for surveillance. It also sells the reports that contain the rating and a detailed description of findings for $750, or $500 to clients which already purchased five or more reports. In addition, it charges clients an annual activation fee of $3,000. A client who buys a report also receives three quarterly updates based on surveillance. The assessment price Moody's charges is roughly equal to its cost of the assessment, and is a fraction of what the accounting firms charge for a similar service[55].

Moody's does not have any sales staff for VIR ratings, but relies on its reputation, word of mouth and pressure the financial institutions put on their vendors.

Challenges

A year into its operations, Moody's has performed a total of around ten assessments[56]. One possible challenge to growth is the focused concern with compliance efforts – detracting from time and money for something that is not a legal requirement or a direct contact with their clients.

To date, Moody's has not been willing to subsidize vendors by charging them below cost or nothing at all for the assessments. The firm felt that money is not the main issue, but the time needed for the assessment itself and for completing the paperwork around it, as the assessments imply dealing with confidential information.

In an attempt to underline the value of its assessments for the vendors, Moody's partnered with Avior Computing, which built Avior Benchmark, a software tool for facilitating compliance with privacy legislation. Once Moody's has performed an assessment, the software maps the covered areas into the applicable privacy legislation requirements, thus eliminating the need for another review of the same issues during a compliance audit.

Moody's has traditionally not been known as a company focused on IT and there has been little interaction between the staff performing the information security assessments and the rest of the company. In addition, as customers for VIR ratings are information security officers, Moody's strong brand has not translated as effective selling point. Of course, when Moody's service is presented to perspective firm's financial organization, the brand recognition is valuable.

[55] According to Ed Leppert, the Big 4 firms charge over $100,000 for such a service (August 14, 2008 interview).
[56] Nye and Leppert, August 11 and 14, 2008, respectively.