# Rankiteo

## Cybersecurity Scoring Model

JULY 2024

A risk management company.
We assess worldwide Cybersecurity.

At the forefront of digital defense, our startup revolutionizes the way businesses understand and manage cyber risk, leveraging the latest technologies for precise quantification. We transform uncertainty into clear metrics, enabling companies to make informed decisions with confidence. Harness the power of cutting-edge innovation to quantify your cyber risk and secure a resilient future in today's fast-paced digital ecosystem.

Rankiteo provides a comprehensive solution to streamline the understanding and management of cybersecurity risks across your entire organization. You have the ability to monitor the security ratings of individual subsidiaries, ensuring that every aspect of your enterprise meets the highest standards of cyber hygiene.

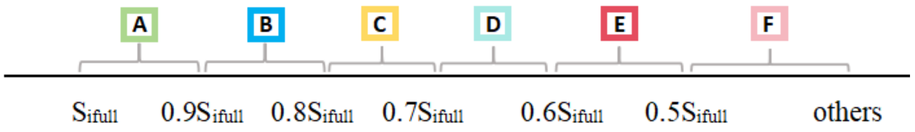
By leveraging key indicators such as DMARC, Certificates Configuration, DKIM Records, SPF Domains, Vulnerability Detection, Web Application Headers, Open Ports, Certificates CVE, Certificates Information, IT Standardization, Digitalization, SBOMs (Software Bill of Materials), and History-Weight, this model provides a comprehensive evaluation of an enterprise’s cybersecurity readiness.

## The Rating Scale

The latest version of Rankiteo includes a rating scale, which has been modified from the previous iteration. This new scale is an A-F scale with an adjusted numeric rating range of 0-1000.

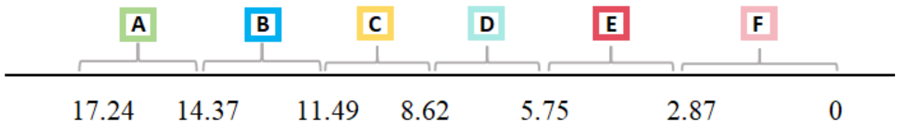
When we have obtained the scores for each module, we also need to convert these scores into grades. Except for the IT Standardization and Digitalization ,  Rankiteo’s rating scale is as follows:

Rankiteo Rating Scale



IT Standardization’s rating scale remains the same as the previous iteration, which is an A-F scale, but the numerical rating ranges are different. We establish a base score based on the number of categories to evenly divide the numerical scoring range.

Digitalization/IT Standardized Rating Scale



## The Objective

The rating model is designed to achieve two objectives: reflect the company's cybersecurity posture and consider the interconnectedness of its subsidiaries.

Reflection of the Company's Cybersecurity Posture

With our detailed breakdown, you can monitor the security ratings of various modules within the company, ensuring that every aspect of your enterprise meets the highest cybersecurity standards. Track your security assessment's completion with real-time updates on remaining items in the queue, empowering you to anticipate the final report and plan your next steps accordingly.

Interconnectedness of Its Subsidiaries

Our cybersecurity scoring platform has the capability to find a wide range of information about your company on the internet, while also respecting the organizational structure of the company's subsidiaries. This means the platform not only identifies vulnerabilities and assesses the cyber health of the main company but also takes into account the interconnectedness and specific roles of its subsidiaries in its overall cybersecurity evaluation.

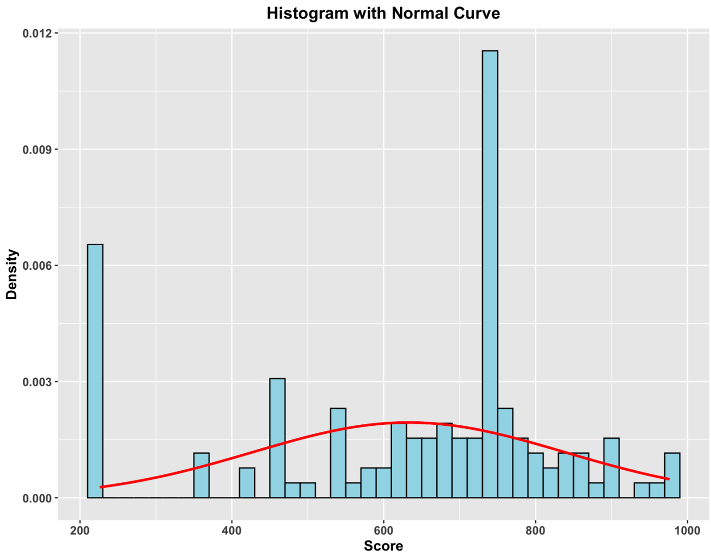
Cybersecurity Dataset

Rankiteo offers the most comprehensive security incident data available. Our proprietary relational database, the Rankiteo Cyber Database, contains information on a wide range of “Cyber risk”-related incidents that have resulted in, or may result in, significant financial judgments or financial losses to business entities.

Organizations with the poorest cybersecurity hygiene (Level F) may have final scores for each module that are approximately 50% of those of Level A. Rankiteo has observed that Level A organizations have exceptionally clean hygiene. For each company, our system automatically analyzes each sub-module to assess its level of cybersecurity. The data from each sub-module is then consolidated.

## Ratings Distribution

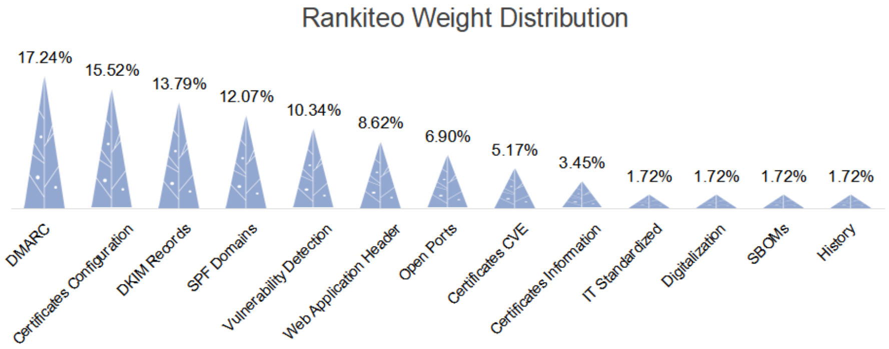
Following a comprehensive evaluation of more than 100,000 companies and their subsidiaries by Raniteo engineers, 31.54% (E or F companies percentage) of organizations were adjudged to be rated as E or F. The mean rating across the entire cohort is 632.9, equating to a D on the A-F scale. A histogram with the fitted normal curve is displayed in the following plot. It is seen that the majority of companies are rated between B and D, which further validates the scoring algorithm.



## Rating Calculation

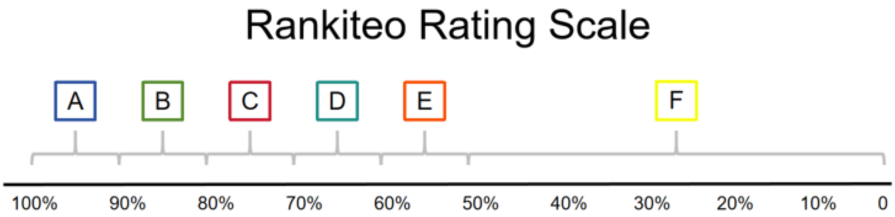
Step 1: Weighting Issues

Rankiteo stores data in modules in a database, acquiring and organizing it in a systematic manner. It aggregates cybersecurity data from thousands of companies to assign appropriate weights to each module based on issue complexity and severity. The differentiation of weighting a given result based on comprehensive cybersecurity information and issue severity is one of Rankiteo's key competitive advantages. This enables us to closely correlate ratings with real-world risk management and risk outcomes. By way of illustration, certificates pertaining to configuration and trust are closely aligned with the level of cybersecurity exhibited by the company in question. Rankiteo assigns a score of 15.52% to the configuration module in this regard.



Step 2: Calculating Module Rating

Each module is evaluated using a specific scoring measure. The optimal score is calculated by combining the module score with the appropriate weighting factor. The relative importance of each module determines the weight assigned to it in the final total score. The risk scores are affected by the weights, and the ratings standardize the level of all modules and final scores. The risk level of each module and the final score is clearly visible to companies. The numerical ratings for each module and the final score are converted to an A-F rating scale, as shown below.



The final ratings of the modules are primarily based on weightings. For instance, the Vulnerability Detection Module has a score of 49, with a weight of 47.37%, which is below 50%. This results in an F rating. However, the final ratings for the IT Standardized Module and the Digitalization Module are provided directly.

> *Please note that the descriptions of the scores and underlying criteria for each module have been simplified by removing details of specific AI and advanced statistical models.*

Bads-Domain Weight: 84.5%

The "bad" rating is determined by a weighted average of each criterion, using the geometric mean for the final calculation. Each finding is weighted according to issue severity and asset value. The rating for each criterion is calculated as follows:

- DMARC-Domain-based Message Authentication, Reporting, and Conformance, which can enhance the security and trustworthiness of email communications. Weight 17.24% of all.
- Certificates Configuration- It refers to the setup and management of digital certificates, which are used to establish secure communications and verify the identity of entities involved in digital interactions. Weight 15.52%.
- DKIM Records-Domain Keys Identified Mail. Less DKIM Records means organizations can significantly improve their email security posture, protecting their brand and users from phishing and spoofing attacks. Weight 13.79% of all.
- SPF Domains-Sender Policy Framework. Optimize the configuration of SPF records to enhance email security and reduce the risk of email spoofing. Weight 14.28% of all.
- SBOMs-Optimize the quantity and quality of Software Bill of Materials to improve software supply chain security. Weight 1.72% of all.
- Web Application Header- Optimize the configuration and implementation of HTTP headers to enhance the security of web applications. Weight 8.62% of all.
- Open Ports- Less number of open network ports that could potentially be exploited by attackers. Weight 6.90% of all.

- Certificates CVE-With less certificates CVE, organizations can take proactive measures to mitigate these vulnerabilities and maintain robust security for their communications and authentication processes. Weight 5.17% of all.

- Certificates Information- Improve the quality and security of certificate management by minimizing issues related to certificates. Weight 3.45% of all.

We encourage engineers to address any bads promptly. If you have resolved any bads, please submit the updates on our website. This will likely result in an improved score compared to the previous evaluation.

Vulnerability Detection-Domain Weight: 10.34%

The Vulnerabilities score is calculated based on the weighted average of severity, impact, and exploitability scores, with the weights applied as follows:

- Severity — Weight 30%.

- Impact—Weight 10%.

- Exploitability—Weight 60%.

We categorize and analyze vulnerabilities based on their severity scores, and the Vulnerability Detection rating is derived from this classification. If companies' engineers resolve more severe vulnerabilities and submit them on our website, your rating will increase rapidly.

IT Standardized-weight: 1.72%

The IT Standardized Module score is based on its rating. We first obtain the rating of the IT Standardized Module and then assign a score based on its rating. For example, a rating of F is assigned a score of 2.87, in ascending order, and a rating of A is assigned a perfect score of 17.24.

Digitalization-weight: 1.72%

The Digitalization Module score is based on its rating and is calculated in the same way as the IT Standardized Module. We first obtain the rating of the Digitalization Module and then assign a score based on its rating. For example, a rating of F is assigned a score of 2.87, in ascending order, and a rating of A is assigned a perfect score of 17.24.

History Vulnerability-weight: 1.72%

The History Vulnerability Module score is calculated based on the total number of vulnerability categories relative to the number of vulnerabilities, with the final score weighted according to the attributes of the vulnerability. We divide the number of history vulnerabilities into 5 categories. A base score is assigned to each category of historical vulnerabilities, e.g. if the number of vulnerabilities in the first category is 0, the base score is full. The score is reduced by 3.448 points for each backward progression of the category. Then, the benchmark score is obtained for each history vulnerability. Finally, a weighted sum of the history vulnerability module scores is calculated based on the vulnerability attribute weights.

Step3:Calculate Module With ‘NA’

If there is a module with no data available, denoted as “NA”, we need to assess it by synthesizing the information contained in other modules with available data. The specific evaluation method is as follows:

- Use the company’s ID to determine historical company data and read the data. This data includes the number of bad modules and the total score, as well as an array of severity values and the total score for the Vulnerability Detection module, and the grade for the IT Standardization module.
- Determine if there are “NA” modules, if so, store their positions, and initialize an array to store the positions of these “NA” modules . Then call functions to calculate the scores of the non-“NA” modules.
- Calculate a new weight based on the existing data to approximate the score for “NA” modules and record them as historical data.

Step 4: Calculate Weighted Module Totals

After calculating the scores for each module, the total sum of the scores for all modules was calculated using the weights shown in the table below and the weights listed in Step 2.

| **Module** | **Weight** | **Example** | **Example Score** |
|---|---:|---:|---:|
| DMARC | 17.24% | 11 | 54.6 |
| Certificates Configuration | 15.52% | 9 | 58.8 |
| DKIM Records | 13.79% | 6 | 67.2 |
| SPF Domains | 12.07% | 10 | 56 |
| Vulnerability Detection | 10.34% | 2(Severity=4.0) | 48 |
| Web Application Header | 8.62% | 0 | 172.41 |
| Open Ports | 6.90% | 0 | 172.41 |
| Certificates CVE | 5.17% | 7 | 64.4 |
| Certificates Information | 3.45% | 6 | 67.2 |
| IT Standardized | 1.72% | A | 17.24 |
| Digitalization | 1.72% | B | 14.37 |
| SBOMs | 1.72% | 6 | 67.2 |
| History | 1.72% | 0 | 17.24 |
| **Total** | 100.00% | **Example Total Score** | 877.07 |

Step 5: Calculate Overall Rating

The final step is to calculate the rank of each module score according to different weights. This is also how the rank of the final total score is calculated. The table below shows an example calculation.

As shown in the table, the final total score and rank are calculated for each module. In addition, the scores and ranks are updated as an organization's security testing results are updated. For example, if an organization fixes its vulnerabilities, its Vulnerability Detection module score will certainly be updated and its rank may be updated. This provides an incentive for organizations to remediate vulnerabilities in a timely manner.

| Module | Weight | Example | Example Score | Example Rank |
|---|---:|---:|---:|---:|
| DMARC | 17.24% | 5 | 70 | F |
| Certificates Configuration | 15.52% | 9 | 52.92 | F |
| DKIM Records | 13.79% | 6 | 53.76 | F |
| SPF Domains | 12.07% | 10 | 39.2 | F |
| Vulnerability Detection | 10.34% | 2(Severity=4.0) | 48 | F |
| Web Application Header | 8.62% | 0 | 86.21 | A |
| Open Ports | 6.90% | 0 | 68.97 | A |
| Certificates CVE | 5.17% | 7 | 19.32 | F |
| Certificates Information | 3.45% | 6 | 13.44 | F |
| IT Standardized | 1.72% | A | 17.24 | A |
| Digitalization | 1.72% | B | 14.37 | B |
| SBOMs | 1.72% | 6 | 6.72 | F |
| History | 1.72% | 0 | 17.24 | A |
| **Total** | 100.00% | **Example Total Score** | 507.39 | E |

## Conclusion

Rankiteo provides a comprehensive platform for visualizing and addressing cybersecurity risks across an entire company and its subsidiaries. This is due to the fact that Rankiteo integrates the cybersecurity hygiene data of each company with data from its related companies. The platform then consolidates this data into a composite rating that is closely aligned with risk assessment outcomes and effective cybersecurity risk management practices. As it is implemented in the real world, you can swiftly identify risk hotspots in individual modules and take action in a timely manner. Furthermore, we provide feedback following the resolution of identified vulnerabilities. Each RiskRecon rating is accompanied by comprehensive assessments that can be shared with vendors to enhance their and your overall risk posture.

Rankiteo instantly assesses your company's cybersecurity health with our dynamic security algorithm. It provides a clear, actionable snapshot of your current security status, enabling you to prioritize and address key areas of concern. At the same time, with our fine-grained segmentation, you can achieve your goal of monitoring the security levels of individual subsidiaries. Our platform visualizes the level of cyber hygiene in every aspect of your organization.