Sustainability

Cyber Risk Score

Methodology & Research Process

July 2026

Version 1.0
PUBLIC DISCLOSURE ON THE METHODOLOGY, MODELS, AND KEY RATING ASSUMPTIONS USED IN ESG RATING ACTIVITIES

ISS STOXX

Contents

Tables & Figures **3**
Tables 3
Figures 3
Regulation (EU) 2024/3005: Public Disclosure on the Methodology, Models, and Key Rating Assumptions Used in ESG Rating Activities **4**
Overview **11**
Scope of the Rating 11
Coverage **12**
Sources of Information **12**
Framework **13**
Cyber Asset Attribution (Curation) 13
DUNS Number 14
Domains 14
IP Network Prefixes 14
Cyber Asset Review (CAR) 15
Findings Collected 15
Industry Classification 16
Data Estimation 17
IP-Based findings 17
Domain-Based Findings 17
Firmographic Findings 17
Scoring Model 18
Model Training 18
Model Response 19
Continuous Scoring 22
Limitations **23**
Quality Assurance **24**
Methodology Review Process **24**
Appendix **25**

Appendix A: Relevant Supporting Models and Key Rating Assumptions 25
Appendix B: Version Control 26

Tables & Figures

Tables

Table 1. Cyber Risk Score Coverage.....12
Table 2. Reason code values and descriptions 21

Figures

Figure 1: Example Cyber Risk Score 19

Regulation (EU) 2024/3005: Public Disclosure on the Methodology, Models, and Key Rating Assumptions Used in ESG Rating Activities

This disclosure is published to meet the relevant requirements of the EU ESG Ratings Regulation (EU2024/3005) and related regulatory technical standards. The following index cross-references to the relevant information are made available within the Cyber Risk Score Methodology Document and on our website.

Within this disclosure, the Regulation (EU) 2024/3005 of the European Parliament and of the Council of 27 November 2024 on the transparency and integrity of Environmental, Social and Governance (ESG) rating activities is referred to as "**Regulation (EU) 2024/3005**".

Within this disclosure, the Commission Delegated Regulation (EU) of 21 04 2026 supplementing Regulation (EU) 2024/3005 of the European Parliament and of the Council with regard to regulatory technical standards specifying the elements of ESG rating products to be disclosed to the public and to users of ESG ratings, rated items and issuers of rated items is referred to as "**Delegated Regulation**".

REGULATION (EU) 2024/3005	DELEGATED REGULATION	REQUIRED INFORMATION	ISS GERMANY AG DISCLOSURE
Rating Product Disclosures			
ANNEX III.1.f	Article 3(1)	ESG rating providers shall disclose information on the ESG rating's clearly defined objective and marking whether the rating is assessing risks, impacts, or both, according to the double materiality principle, or any other dimensions, and in the case of double materiality the proportion of the risk and impact materiality. ESG rating providers shall disclose at the level of each ESG rating product: a) a description of the risks covered, where the ESG rating is assessing risks; b) a description of the impacts covered, where the ESG rating is assessing impacts; c) information on how the risk and impact materiality are taken into account according to the double materiality principle, where applicable; d) where the ESG rating is based on other materiality dimensions, a description of those dimensions.	Please refer to: • Overview
ANNEX III.1.g	Article 3(2)	ESG rating providers shall disclose the ESG rating's scope, namely, whether it covers an individual E, S, or G factor or whether it is an aggregated rating aggregating E, S and G factors, or whether it covers specific issues such as transition risks. ESG rating providers shall disclose at the level of each ESG rating product: a) a description of what is covered under the E, S or G factors and which factors are aggregated, where applicable; b) a description of the specific issues that the ESG rating covers.	Please refer to: • Overview

REGULATION (EU) 2024/3005	DELEGATED REGULATION	REQUIRED INFORMATION	ISS GERMANY AG DISCLOSURE
ANNEX III.1.h	N/A	ESG rating providers shall disclose in the case of an aggregated ESG rating, the weighting of the three overarching E, S and G categories of factors (for example 33 % for the E factor, 33 % for the S factor, 33 % for the G factor), and the explanation of the weighting method, including weight per individual E, S and G category.	• This requirement is not applicable to the Cyber Risk Score.
ANNEX III.1.i	N/A	ESG rating providers shall disclose within the E, S or G factors, specification of the topics covered by the ESG rating, and whether they correspond to the topics from the sustainability reporting standards developed pursuant to Article 29b of Directive 2013/34/EU.	Please refer to: • Overview
ANNEX III.1.j	N/A	ESG rating providers shall disclose information on whether the rating is expressed in absolute or relative value.	Please refer to: • Overview
ANNEX III.1.o	Article 3(3)	ESG rating providers shall disclose if an ESG rating of a rated item covers the E factor, information on whether that rating takes into account the targets and objectives of the Paris Agreement or any other relevant international agreements. ESG rating providers shall disclose if an ESG rating of a rated item covers the S and G factors, information on whether that rating takes into account any relevant international agreements. ESG rating providers shall at the level of each ESG rating product: a) include an indication of whether the ESG rating takes into account the targets and objectives of the Paris Agreement and which other international agreements are considered, with reference to basic identifying information on these agreements together with an explanation of their relevance to the ESG rating; b) specify whether the ESG rating is assessing alignment of commitments against the objectives of the agreements referred to in point (a).	Please refer to: • Overview
ANNEX III.1.p	Article 3(4)		

REGULATION (EU) 2024/3005	DELEGATED REGULATION	REQUIRED INFORMATION	ISS GERMANY AG DISCLOSURE
Basic Methodological Disclosures			
ANNEX III.1.a	Article 4(1)	ESG rating providers shall disclose an overview of the rating methodologies used and changes thereto, including whether analysis is backward-looking or forward-looking and the time horizon covered. ESG rating providers shall disclose: a) the title of the rating methodology used; b) a description of the types of rated items in relation to which the methodology referred to in point (a) applies; c) the time horizon over which the ESG rating is considered valid, where applicable d) a list and overview of the relevant supporting models and key rating assumptions, where applicable; information on measures and procedures to ensure the quality and reliability of data used; e) a description of the defined ranking system of rating categories used, with reference to: i. the meaning of each rating category for absolute and relative values and how the ranking system should be interpreted; ii. in the case of relative values, an explanation as to whether they are relative to a specific industry, geographical area, peer groups or other comparative references and their respective description. f) the dates of the most recent update of the methodology and a description of the changes introduced to the previous version.	Please refer to: Points a) and f) • Appendix B: Version Control Points b) to e) • b) Overview, Coverage • c) Overview, Continuous Scoring • d) Scoring Model, Appendix A: Relevant Supporting Models and Key Rating Assumptions, Quality Assurance • e) Model Response

REGULATION (EU) 2024/3005	DELEGATED REGULATION	REQUIRED INFORMATION	ISS GERMANY AG DISCLOSURE
ANNEX III.1.b	Article 4(2)	ESG rating providers shall disclose the industry classification used. ESG rating providers shall provide: a) the name of the issuing body of the industry classification used; b) the name and version of the industry classification used; c) any publicly available link to the official documentation of the industry classification system.	Please refer to: • Industry Classification
ANNEX III.1.c	Article 4(3)	ESG rating providers shall disclose an overview of data sources, including whether data is sourced from sustainability statements required under Directive 2013/34/EU or from information disclosed under Regulation (EU) 2019/2088 and whether sources are public or non-public, and an overview of data processes, estimation of input data in case of unavailability and frequency of data updates. ESG rating providers shall include a description of the engagement process with rated items or issuers of rated items, including how the input from such engagement is taken into account.	Please refer to: • Data Sources: Sources of Information • Data Process: Framework • Estimation of Input Data: Data Estimation • Frequency of Data Updates: Continuous Scoring • Engagement with rated items or issuers of rated items is not part of the Cyber Risk Score process.
ANNEX III.1.e	Article 4(4)	ESG rating providers shall disclose information on whether and how the rating methodologies are based on scientific evidence. ESG rating providers shall where applicable, describe the process for identifying relevant scientific evidence.	Please refer to: • Scoring Model

REGULATION (EU) 2024/3005	DELEGATED REGULATION	REQUIRED INFORMATION	ISS GERMANY AG DISCLOSURE
ANNEX III.1.k	N/A	ESG rating providers shall disclose where applicable, reference to the use of artificial intelligence in the data collection or rating process including information about current limitations and risks of using artificial intelligence.	Please refer to: • Scoring Model
Limitations in data sources, methodologies and information			
ANNEX III.1.m	Article 5	ESG rating providers shall disclose any limitation in data sources and methodologies used for the construction of ESG ratings. ESG rating providers shall disclose any limitation on the information available to ESG rating providers.	Please refer to: • Limitations • Limitations to Methodologies & Data
ANNEX III.1.q	Article 5	ESG rating providers shall explain any limitations in respect of the following: a) the availability or consistency of data used in the rating process; b) the completeness, timeliness and accuracy of information; c) the use of assumptions, proxy reference points and data estimation.	
Organisational Disclosures			
ANNEX III.1.d	Article 6(2)	ESG rating providers shall disclose the ownership structure of the ESG rating provider. ESG rating providers shall disclose: a) a chart illustrating their ownership links with any parent undertaking and subsidiaries. The chart shall indicate, where applicable, whether any of those entities perform any of the activities listed in Article 16 (1) or services referred to in Article 16(6) of Regulation (EU) 2024/3005.	Please refer to: • Ownership Structure

REGULATION (EU) 2024/3005	DELEGATED REGULATION	REQUIRED INFORMATION	ISS GERMANY AG DISCLOSURE
ANNEX III.1.l	Article 6(3)	ESG rating providers shall disclose general information on criteria used for establishing fees charged to clients, specifying the various elements taken into consideration, and general information on the business/payment model. ESG rating providers shall disclose the following: a) how the criteria they apply for establishing fees ensure that fees are fair, reasonable, transparent and non-discriminatory in accordance with Article 27 of Regulation (EU) 2024/3005; b) whether the ESG rating provider operates a subscription-paid model, an issuer-paid model, a combination of those models, or another model; c) a description of the relevant business model, and the proportion of total annual revenue derived from each model; d) where applicable, the impact of fees charged for services other than ESG rating activities on the determination of fees for ESG ratings, together with a description of those other services.	Please refer to: • Pricing Policy
ANNEX III.1.n	Article 6(1)	ESG rating providers shall disclose the main risks of conflicts of interest and the steps take to mitigate them. ESG rating providers shall indicate the areas of the ESG rating provider's activities, services or organisational structure from which the main risks of conflicts of interest may arise.	Please refer to: • Conflict of Interest Policy

Overview

The **ISS STOXX Cyber Risk Score** is a data-driven scoring and screening solution that provides an opinion on companies' management of cybersecurity risks. The Score itself is a concise, empirical, and proactive metric that indicates how effectively a company manages and maintains its network security, powered by a machine learning model trained to identify the potential for a breach event.

The **Cyber Risk Score** is forward-looking and represents the likelihood that an organization will suffer a material cyber incident (e.g., breach) within the next 12 months, expressed as a score on a scale from 300 to 850. The Cyber Risk Score scoring model is trained to recognize patterns and signals indicative of breach risk. A historical dataset with known breach outcomes is used for model training. Records of cybersecurity breach incidents are continuously identified by ISS STOXX and used to identify affected organizations and the corresponding timeline of breach incidents.

A score of 300 represents high risk; a score of 850 represents lower risk. A company with a Cyber Risk Score closer to 300 is assessed to be at significantly higher risk of experiencing a material cyber incident in the next 12 months than is a company with a Cyber Risk Score closer to 850. The overall Cyber Risk Score is expressed as an absolute value, based on a fixed scoring scale, and does not depend on peer, sector, or universe-relative comparisons. The Cyber Risk Score is accompanied by complementary outputs including the Cyber Risk Decile and Cyber Governance & Management Decile, both of which are expressed in relative values.

The **Cyber Risk Score** is calculated based on the behavior of an organization, as well as firmographic information that includes company size and the industry in which the firm operates. Organizational behaviors are assessed through an array of IP and domain-based data collections.

Each company's **Cyber Risk Score** is generated from data findings collected from cyber assets identified as being either owned or operated by the company or any of the company's majority-owned subsidiaries. (Cyber asset attribution is covered in more detail later in this document.) Each company's asset attribution is reviewed at least annually, while each week a new score is generated based on findings collected over the previous week. Historical scores and data provide greater context and trend analysis to understand a company's approach to managing cyber risk over time.

Scope of the Rating

The Cyber Risk Score assesses cyber risk which can be considered a Governance (G) factor. It does not incorporate Environmental (E) or Social (S) factors and accordingly does not take into account the targets and objectives of the Paris Agreement or any other international agreements. The topics covered by the Score do not correspond to the sustainability reporting topics under Article 29b of Directive 2013/34/EU.

Coverage

While any company with any level of internet-based operation can be assessed and scored by the Cyber Risk Score platform, the ISS STOXX data team maintains a set of pre-curated or pre-profiled companies. Cyber Risk Score coverage comprises approximately 4000 companies in the United States.

Table 1. Cyber Risk Score Coverage

ISS STOXX CONTEXT	COUNTRY	COVERAGE
DataDesk	United States, Canada, Australia	S&P 500, S&P 400, S&P 600, Russell 3000, TSX 250, and ASX 300 Indices
Proxy Research Report	United States, Canada, Australia	S&P 500, S&P 400, S&P 600, Russell 3000, TSX 250, and ASX 300 Indices

Sources of Information

The Cyber Risk Score relies on three primary categories of data:

1. Firmographic data from Dun & Bradstreet, including industry classification and company size;
2. Domains owned or operated by the company, which are used for web and DNS configuration assessment; and
3. IP network prefixes attributed to the company, which support the collection of endpoint-, infrastructure-, and network-level observations.

Historical cybersecurity incident data, sourced from publicly available legal and regulatory disclosures, including US state-level breach notifications, company filings, and SEC filings such as Form 8-Ks and Form 10-Ks, is also used for model training and validation.

In addition, the Cyber Governance & Management Decile focuses on governance and management practices, drawing on inputs from ISS STOXX Governance QualityScore and publicly available company disclosures to assess cybersecurity oversight, risk management, and related governance structures across peer groups.

The Cyber Risk Score does not use sustainability statements required under Directive 2013/34/EU and does not incorporate disclosures under Regulation (EU) 2019/2088 (SFDR). All sources used in the methodology are either public or commercially licensed datasets.

Framework

The Cyber Risk Score works by identifying a company's cyber assets, collecting data from or about those assets, and submitting the collected data findings to a machine learning model for scoring.

Scoring any company is a three-step process:

1. **Cyber Asset Attribution (Curation)**
   Identify and attribute the cyber assets of a company:
   a. Dun & Bradstreet Number
   b. Domains
   c. IP Network Prefixes (i.e., blocks of IP addresses)
2. **Collect Data Findings**
   Collect and compile findings from and about the cyber assets on a weekly basis
3. **Score Findings by Machine Learning Model**
   Submit collected findings to the machine learning scoring model, which returns the Cyber Risk Score, Firmographic Max, and top three reason codes.

Cyber Asset Attribution (Curation)

In the context of the Cyber Risk Score, cyber asset attribution is also referred to as "curation." Curation in this context refers to the identification of cyber assets owned or operated by the company, and the company's majority-owned subsidiaries, that are to be scored.

An organization's Cyber Risk Score is calculated in part from indicators based on observations of its public internet-based properties, which include domains and IPv4 network prefixes owned by the organization. Most of the indicators that contribute to the organization's score are based on observations associated directly with these assets, such as websites being served on their respective domains, or malicious behavior observed from IP addresses from the organizations attributed network prefixes.

There are 3 key cyber assets identified for each company in the curation (cyber asset attribution) process:

1. **DUNS number** – The Dun & Bradstreet number that most accurately identifies the company being scored.
2. **Domains** – The active internet domains that the company being scored owns or operates.
3. **IP Network Prefixes** – The active IP addresses allocated to the company being scored by their RIR (Regional Internet Registry). A "prefix" is defined as a block of IP addresses expressed in CIDR notation (e.g., a.b.c.d/n).

The curation process aggregates data collected from each of the three cyber assets above to assemble a company's complete cyber profile.

DUNS Number

ISS STOXX uses Dun & Bradstreet firmographic data to pull in each company's firmographic information, including specifically industry and company size, as measured by employee count.

Domains

One of the primary identifiers of a company's cyber assets is the set of Internet domains registered to them. Each company's domains typically serve as a virtual "front door" to the overall enterprise or even potentially to a set of specific products or services. Websites hosted at publicly accessible domains serve as another public cyber asset available to ISS STOXX for risk analysis.

Just as with other externally observable cyber assets, the overall management and ongoing maintenance of each company website serves as a signal of possible risk. The ISS STOXX domain-based web crawler collects data that captures the risk in the construction, configuration, and content of an organization's externally accessible web instance(s).

In addition to providing the Cyber Risk Score platform with the information needed for crawling each company's publicly available websites for risk signals, domains also serve as a primary means by which to look up the score of each company.

IP Network Prefixes

ISS STOXX's source of authority for IP network attributions are the Regional Internet Registries (RIRs). There are five RIRs in the world. RIRs receive address space in large blocks from the Internet Assigned Numbers Authority (IANA) and allocate smaller address blocks to organizations within their regions. These organizations then assign IP addresses to consumers. RIRs manage, distribute, and register Internet number resources (IPv4 and IPv6 address space and Autonomous System (AS) Numbers) within their respective regions.

RIRs maintain databases that contain detailed records of which resources have been allocated and assigned, as well as which organizations and POCs (points of contact) are authoritative over those resource records. In addition to being referred to as RIR data, it is often more commonly referred to as "WHOIS data," pronounced "who is data." ISS STOXX aggregates this publicly available IP registry WHOIS data from all five RIRs to then serve as the single source of record used to attribute IP space to companies for scoring.

Companies may, as part of standard business practices, reallocate or reassign some or all of their allocated IP space to another company for that other entity's exclusive use and control. The RIRs strongly encourage that such transfers be officially documented within the appropriate RIR registry and provides a variety of resources to aid in registering reassignments. Doing so not only adheres to the general principles and intent of the RIRs, to serve as the public record of global IP address space usage, but also provides the mechanism through which changes in asset attribution are communicated to ISS STOXX.

The Cyber Risk Score cyber asset attribution (a.k.a. "curation") methodology is written to ensure a consistent and uniform approach that is applied fairly to all scored organizations. In cases where an organization subleases their own IP network space that has been allocated or assigned to them by an RIR, ISS STOXX will continue to attribute that IP network space to the lessor, rather than the lessee, unless and until the transfer has been properly registered.

Cyber Asset Review (CAR)

The Cyber Asset Review process allows companies to review the collection of the curated assets which define the company's external footprint. Through this process, companies can identify any cyber assets (domains or IP networks) that they believe should be added or removed from their company profile.

While ISS STOXX takes great care in the development and adherence to the Cyber Risk Score cyber asset attribution methodology, ISS STOXX encourages all companies to review their own Cyber Risk Score and the cyber assets that have been attributed to them for scoring.

Every company is invited to log in to the Cyber Risk Score platform to review their attributed cyber assets for accuracy and completeness. Companies may submit any change requests directly within the platform and those change requests will then be reviewed by the ISS STOXX data team, according to the Cyber Risk Score cyber asset attribution methodology.

Findings Collected

The Cyber Risk Score model produces a score based on a diverse dataset collected regularly by ISS STOXX. This dataset incorporates elements indicative of organizational security posture on endpoints, software and services, and infrastructure configuration. The rate at which various data sources are refreshed in the Cyber Risk Score portal ranges from daily to weekly. All profiled companies are re-scored weekly.

The complete set of data findings collected and used in scoring are listed here:

IP-based findings

- **Internet Presence**
  - ICMP Responders
- **Endpoints**
  - Spam
  - Malware
  - Scanning
- **Infrastructure**
  - Network Time Servers

    - Misconfigured DNS
- **Software Services**
    - Alternative Web Servers
    - Public Databases
    - Unsecure Remote Access
    - Misconfigured SSL
    - Remote Login Servers

Domain-based findings

- **Websites**
    - Inline JavaScripts
    - Software Headers

Firmographic findings

- **Industry**
- **Employee Count**

Industry Classification

The industry classification used in the Cyber Risk Score is sourced from Dun & Bradstreet firmographic data. Each company is assigned a Standard Industrial Classification (SIC) code, which is mapped to the internal ISS STOXX industry grouping structure used in the model. The SIC codes applied are based on the most recent version of the Standard Industrial Classification system maintained by Dun & Bradstreet.

Industry Classification

- Agriculture and Food
- Business Services
- Construction
- Energy and Utilities
- Finance and Banking
- Healthcare

- Materials and Manufacturing
- Media, Telecom and Technology
- Retail and Consumer Services
- Transportation

Data Estimation

The Cyber Risk Score does not use estimated, proxy, or imputed data. All input data, whether domain-based findings, IP-based findings, or firmographic attributes, is based solely on direct observations or authoritative sources such as Dun & Bradstreet and Regional Internet Registry WHOIS data.

IP-Based findings

Data reflecting malicious behavior and botnet activity consists of daily recordings of IP addresses engaging in malicious activities, such as sending out spam, participating in phishing and/or malware schemes, and unsanctioned port scanning. These data reflect malicious behavior at the level of individual endpoints within an organization's network, regardless of any peculiarities of the network itself. Publicly available reputation blacklists reflect common behaviors; a sound organizational security posture includes prompt investigation and remediation of addresses appearing on these lists within the organization's managed IP space.

Measurements of an organization's external attack surface, vigilance in configuring public-facing network assets to conform to standard best practices, vulnerability to existing exploits, and propensity to vulnerability to additional exploits are taken at a regular cadence, at the address level. Such measurements are indicative of the organizational security posture both directly and indirectly. These data reflect both the overall size of the attack surface and service- and function-specific configuration issues. Common but serious misconfigurations, such as expired or invalid SSL/TLS certificates presented by endpoints when attempting to establish a secure connection over an application protocol such as HTTPS or SSH, are measured and used to inform the endpoint's contribution to the overall attack surface.

Domain-Based Findings

Regular snapshots of an organization's public-facing website(s) are used to measure risk associated with web-based attacks themselves and with the degree of adherence to best practices. Keeping a website aligned with current best practices is indicative of a strong security posture. By minimizing exposure of underlying infrastructure, site owners give would-be attackers less information about software vulnerabilities. Restricting use of web resources to those obtained from trusted sources can mitigate clickjacking and cross-site scripting attacks. Web data are used to calculate breach risk that is attributed to an organization's web presence.

Firmographic Findings

Firmographic data, such as industry classification, may also be taken into consideration in producing a score from the Cyber Risk Score model. These data are utilized to account for inherent risk that's introduced by industry and organizational factors.

Scoring Model

The Cyber Risk Score methodology is empirical and data-driven. As such, it is not based on scientific evidence. The machine learning model is trained using historical cybersecurity incidents and associated asset-level observations, enabling the model to identify statistical patterns linked to elevated breach risk. The empirical evidence supporting the methodology consists of validated historical breach outcomes and the corresponding network and domain attributes observed during the pre-incident period.

Every company is scored by the same scoring model. ISS STOXX retrains and releases an updated scoring model on an annual basis. This allows the Cyber Risk Score analytics team to review and retest the predictive qualities of the data finding features used in scoring as well as re-train the model on the latest known cyber breach data.

The analytic model constituting the scoring engine of the Cyber Risk Score solution is trained to recognize patterns and signatures indicative of breach risk. A historical dataset with known breach outcomes is used for model training. Records of cybersecurity breach incidents are continuously identified by ISS STOXX and used to identify affected organizations and the corresponding timeline of breach incidents.

In compiling the model development dataset, a recent time period of one year is selected. The organizations affected by significant cybersecurity breach incidents over the course of the following year are added to the set of victim organizations. Another set of organizations is created from the pool of organizations that, to the best of our knowledge, did not suffer a significant cybersecurity breach incident over the course of the following year (i.e., the year immediately after the selected one). These two pools of “breach victim” organizations and “unbreached” organizations respectively are used to create the model development dataset.

The dataset itself is constructed by selecting, for each organization individually, an “observation date” within the 12 months immediately preceding the breach incident, extracting the data associated with the organization’s internet-based properties at that point in history, and using it to create a data record to be scored by the model. Nominally, these internet-based properties comprise all IPv4 prefixes delegated to the organization by the appropriate numbering authority (typically one of the Regional Internet Registries), the set of pay-level or top-level domains registered to the organization, and the observed internet behavior associated with each. As the notion of “ownership” in this context is sometimes unclear, significant effort is exerted in this crucial aspect of building the development dataset, in order to ensure the mappings of internet properties to organizations is as accurate as possible.

Model Training

The Cyber Risk Score is calculated using variables based on the organization’s network and domains, and on the organization’s riskiest sub-organization networks. The variables used are expert features designed to expose and amplify various factors contributing to breach risk across different data channels and their changes over time. ISS STOXX combines its deep analytics capabilities with world-class cybersecurity expertise to build an exhaustive set of variables that defines a space in which the highest number of potential risk indicators are exposed in as explicit a manner as possible.

This space set of variables is then filled with ISS STOXX’s historical dataset with known outcomes. The model is trained on this data, discarding irrelevant variables and learning new, powerful relationships as it improves.

The trained model's performance is then measured empirically against a holdout sample of data which was not utilized in the model training set.

Model Response

The scoring model returns the following outputs:

- Cyber Risk Score
- Firmographic Max
- Reason Codes
- Incident Type Likelihood

Cyber Risk Score

The **Cyber Risk Score** is a 3-digit score ranging from 300 to 850. The Cyber Risk Score is a predictive score representing an organization's odds of suffering a material breach within the next 12 months based on their external security posture and cyber hygiene indicators. A score of 300 presents an organization most at risk of suffering a material breach within the next 12 months, and a score of 850 being least at risk of suffering a material breach within the next 12 months.

Figure 1: Example Cyber Risk Score

Firmographic Max

The **Firmographic Max** for any given organization is the highest Cyber Risk Score possible for the company, even in the absence or complete remediation of any IP or domain level findings. In other words, the Firmographic Max represents the fixed or inherent risk that is introduced by industry and organizational factors, such as the size of the company measured by employee count, that cannot be remediated.

Cyber Risk Decile

The Cyber Risk Decile is a relative classification that places companies into ten risk categories based on their Cyber Risk Score in relation to peers. The decile ranking provides an indicative comparison of a company's cyber risk position within its relevant peer group, where Decile 1 reflects comparatively lower assessed cyber risk and Decile 10 reflects comparatively higher assessed cyber risk.

The decile classification is derived from the relationship between a company's Cyber Risk Score and its Firmographic Max, which reflects inherent risk factors related to company size and sector. Decile rankings are calculated within relevant peer groupings, with adjustments to account for differences in company size, sector, and coverage universe.

Cyber Governance & Management Decile

The Cyber Governance & Management Decile is a relative, decile-based classification that reflects a company's cyber governance and management practices in comparison to peers. The assessment considers governance-related factors associated with information security risk oversight and information security risk management and is derived from the Governance Quality Score (GQS) framework, using underlying data from the Information Security Risk Oversight and Information Security Risk Management components.

Companies are positioned into deciles based on aggregated governance-related indicators, where lower deciles indicate comparatively stronger governance practices and higher deciles indicate comparatively weaker practices. These outputs are provided for comparative and analytical purposes and do not represent standalone ESG ratings.

Reason Codes

The Cyber Risk Score model assesses organizational security posture across a wide range of indicators and provides a set of reason codes that provide insight into the factors most impacting the score. The reason codes should be treated as general characteristics of present and historical security posture that can be applied to broad organizational activities rather than specific malicious activity.

The scoring model always returns the top three **reason codes** contributing to the score, regardless of the risk level of the score. These top three reason codes are always returned in rank order from greatest score impact to least.

The reason codes broadly capture three types of risk indicators: risky endpoint activity, risky software and service practices, and risky infrastructure configuration.

Table 2. Reason code values and descriptions

REASON CODE	DESCRIPTION
105	DNS misconfigurations
110	Exposure of internal services
111	Certificate management
112	Proxy configuration and internal web services
113	Attack surface
114	Endpoint malicious activity
115	Remote access services
116	Exposed database services
117	Data transfer services
118	Human attack surface
119	Sector risk
120	Exposure of internal services by the poorest network prefix
121	Certificate management of the poorest network prefix
122	Proxy configuration and internal web services of the poorest network prefix
123	Attack surface of the poorest network prefix
124	Endpoint malicious activity of the poorest network prefix
125	Remote access services of the poorest network prefix
131	Webserver configuration
134	Webserver attack surface and observability
135	DNS misconfigurations

Incident Type Likelihood

The **Incident Type Likelihood** represents the likelihood that specific types of cyber incidents will occur if a cyber-attack takes place.

The *Incident Type Likelihood* scores below provide a comparative assessment of how likely each of these five major cyber incident types is to occur within this organization, in the event of a significant cyber incident.

It evaluates five major incident types:

- Human Error
- Malware & Ransomware
- Social Engineering & Phishing
- Third Party
- Vulnerability Exploit

Each incident type is listed with a likelihood score from 1 to 10, with higher scores indicating greater probability. These scores are derived from firmographic data—such as industry sector, organizational size (by employee count and revenue)—and reflect patterns observed across similar organizations. Technical signal data is not used in the formulation of these scores.

Importantly, this feature is independent of the overall likelihood of experiencing a significant cyber incident, which is captured separately in the organization's ISS Cyber Risk Score.

This insight is intended to help leadership and risk teams prioritize threat scenarios, tailor mitigation strategies, and allocate resources more effectively.

Continuous Scoring

Scoring data is collected at least once a week and a new Cyber Risk Score is recalculated for every scored company. Accordingly, the Cyber Risk Score is considered valid until the next scheduled update. This allows *continuous monitoring* of one's own Cyber Risk Score as well as those under continuous monitoring for vendor management, insurance underwriting and ongoing investment decisions.

Limitations

The Cyber Risk Score's methodology and data may be subject to certain limitations. The below outlines such limitations as well as the action taken to address these:

Limitations in Availability or Consistency of Data Sources

- The Cyber Risk Score is based on externally observable asset-level data, which may vary in availability across organizations depending on their public-facing infrastructure.

Limitations in the Completeness, Timeliness, and Accuracy of Information

- Completeness and timeliness of underlying data are influenced by changes in domain registrations, IP allocations, and publicly observable configurations.

Limitations in the use of Assumptions, Proxy Reference Points, and Data Estimation

- While the Score relies solely on direct observations and authoritative records, gaps may arise where assets are not externally visible. However, the methodology does not use assumptions, proxy reference points, or estimated data.

Limitations and risks of using artificial intelligence

- The Cyber Risk Score is generated by a proprietary machine learning model. While the model is trained on historical data and validated using established analytic techniques (including the use of hold-out samples, retro-analyses, and period out-of-band validations), its outputs are subject to certain limitations, including sensitivity to potential bias in the training data (for example, due to the self-reported nature of the incident outcomes used to train the supervised model).

- Model performance may vary over time due to changes in threat landscapes, trends in cyber incidents, exposure of new vulnerabilities, and organizational behavior. These items, and others, may reduce alignment with patterns observed during model training.

- The model identifies statistical relationships between risk signals and incident outcomes, but does not establish causation; therefore, it should be interpreted as a probabilistic assessment rather than a deterministic prediction.

- To mitigate these risks, the model is subject to periodic review, retraining, and performance monitoring, and operates within a controlled methodological framework based on observable and verifiable data inputs.

Quality Assurance

The Cyber Risk Score incorporates several controls to ensure data quality and reliability. Cyber asset attribution relies on authoritative IP ownership data from Regional Internet Registries. Data findings are refreshed daily to weekly depending on source type, and all covered companies are rescored weekly. The scoring model is retrained annually using updated breach data and evaluated through holdout validation procedures to confirm predictive performance.

Methodology Review Process

The Cyber Risk Score methodology is subject to periodic reviews and updates that are overseen by ISS STOXX's Sustainability Methodology Review Board which comprises experienced methodology and research leaders across jurisdictions.

The solution's underlying methodology is considered valid until an update is carried out and applied. Triggers of methodology update include updates from input data sources, technical developments, and feedback from internal and external stakeholders. Relevant upcoming methodology changes are communicated to clients on a yearly basis.

Appendix

Appendix A: Relevant Supporting Models and Key Rating Assumptions

Models

- **Cyber Risk machine learning model**: Produces a forward-looking score representing the likelihood of a material cyber incident within the next 12 months, trained on historical breach outcomes and associated observations.

Assumptions

- **Asset-based observation premise**: Assumes external observable properties (domains and IP prefixes) and their measured behaviours/misconfigurations are indicative of security posture and breach risk.

- **Attribution premise**: IP space remains attributed to the registered entity (lessor) unless transfer is registered in RIR.

Appendix B: Version Control

Name of Methodology: Cyber Risk Score

VERSION	DATE	DETAILS
1.0	July 2026	Publication of the Cyber Risk Score Methodology and Research Process document Inclusion of the Public Disclosure on the Methodology, Models, and Key Rating Assumptions Used in ESG Rating Activities (as defined by the Regulation (EU) 2024/3005)

ISS STOXX

sales@iss-stoxx.com
iss-stoxx.com

ISS STOXX delivers world-class research, data, and technology solutions that empower capital market participants to pursue their visions with confidence. Our expertise spans indices, corporate governance, sustainability, cyber risk, and fund intelligence, giving clients the tools they need to uncover opportunities, manage risks, and navigate evolving regulations. We are made up of 4,000 professionals operating across 20 countries and serving approximately 5,000 clients, including many of the world's leading institutional investors. Our scale and reach give us deep market knowledge, while our innovative methodologies allow us to offer our clients tailored insights that drive impact and success.

ISS STOXX Sustainability enables investors to develop and integrate responsible investing policies and practices, engage on responsible investment issues, and monitor portfolio company practices through screening solutions. It also provides climate data, analytics, and advisory services to help financial market participants understand, measure, and act on climate-related risks across all asset classes. In addition, our Sustainability solutions cover corporate and country research and ratings enabling its clients to identify material social and environmental risks and opportunities. Sustainability solutions are provided by Institutional Shareholder Services Inc., an investment adviser registered under the U.S. Investment Advisers Act of 1940.