

# Sustainable Accounting Standards Board (SASB) Metrics

**Table 1. Sustainability Disclosure Topics & Accounting Metrics**

Code	Metric	2021 Performance	
<b>Transparent &amp; Efficient Capital Markets</b>			
FN-EX-410a.1	(1) Number and (2) average duration of (a) halts related to public release of information and (b) pauses related to volatility	<b>Number</b>	<b>Duration</b>
		<b>Halt</b>	News event trading halts: NYSE: 268 NYSE American: 33 NYSE Arca: 6
		<b>Pause</b>	The duration of material news-related trading halts fluctuates on a case-by-case basis and can be anywhere from a few minutes to a few hours or even a few days.  LULDs (or single-stock circuit breakers): NYSE: 515 NYSE Arca: 61 NYSE American: 368
FN-EX-410a.2	Percentage of trades generated from automated trading systems	We operate securities and futures exchanges. None of the members of our securities exchanges are required to disclose whether orders sent are generated by automated trading systems and thus ICE cannot track this information. In our futures exchanges, the requirement to identify usage of an automated trading system varies by jurisdiction and the percentage of trades generated by any version of an automated trading system varies by asset class and can range greatly in any given product / instrument.  Automated trading in securities and futures markets provides more liquidity, increases capacity for market making, and results in more efficient price discovery through tighter bids and offers. Risks include the potential for operational and technology disruptions, which we mitigate via robust protocols for risk management, disaster recovery / business continuity and market surveillance.	
FN-EX-410a.3	Description of alert policy regarding timing and nature of public release of information	The NYSE Timely Alert procedures(1) for listed companies apply between the hours of 7:00 am ET and 4:00 pm ET. NYSE-listed companies are required to use any Regulation FD compliant disclosure method (2) to disseminate material news to the public (including foreign private issuers even though not subject to Regulation FD). Companies are required to follow the procedures below:  1. Between the hours of 7:00 am and 4:00 pm (3), companies are required to call the NYSE at least 10 minutes in advance of issuing material news or news that might impact trading in the company's securities. Outside of these hours, companies are not required to provide advance notice to the NYSE, but are encouraged to email a courtesy copy of the news if it is material.  2. When providing the 10-minute advance notice, companies should direct their call to the NYSE Market Watch team at 877.699.2578 or 212.656.5414. When calling, it is important that the company's representative be knowledgeable about the details of the news being issued.  3. In advance of issuing the news, the company must submit a copy of the press release or other Regulation FD disclosure to the NYSE. The disclosure can be submitted in one of two ways; (1) upload the document to Listing Manager or (2) email to nysealert@nyse.com. In addition, companies are required to provide a representative's contact	

		<p>information in case questions arise, and if providing via email, to include in the subject line: ticker symbol followed by a hyphen and the headline of the press release (example: XYZ-XYZ Corp. Announced First Quarter Earnings).</p> <p>4. In order to allow for the orderly closing of a company's stock on the NYSE, companies are prohibited from publishing material news after the official closing time for the NYSE's trading session until the earlier of 4:05 p.m. ET or the publication of the official closing price of the listed company's security (except when publicly disclosing material information following a nonintentional disclosure in order to comply with Regulation FD). The NYSE continues to encourage companies to hold post-market news releases until 4:15 p.m.</p> <p>Footnotes:  (1) The full text of the timely alert policy can be found in Section 202.06 of the NYSE Listed Company Manual for NYSE listed issuers; Section 401 of the NYSE American Company Guide for NYSE American listed issuers; Rule 5.3-E(1)(2) of the NYSE Arca Company Guide for NYSE Arca listed issuers.</p> <p>(2) The full text of Regulation FD is available at <a href="https://www.sec.gov/rules/final/33-7881.htm">https://www.sec.gov/rules/final/33-7881.htm</a>.</p> <p>(3) NYSE Regulation will only implement news pending trading halts upon a company's request between the hours of 7:00am ET and 9:30am ET.</p> <p>Additional details can be found in Section 202.05, 202.06, and 202.07 of the NYSE Listed Company Manual</p>
FN-EX-410a.4	Description of policy to encourage or require listed companies to publicly disclose environmental, social, and governance (ESG) information	<p>The NYSE provides resources and tools to encourage and help issuers build out their ESG disclosure program, including reporting guidance, ESG data disclosure and benchmarking tools, networking groups, webinars, newsletters, and other educational content.</p> <p><b>NYSE ESG Resource Center</b> →</p>
<b>Managing Conflicts of Interest</b>		
FN-EX-510a.1	Total amount of monetary losses as a result of legal proceedings associated with fraud, insider trading, anti-trust, anti-competitive behavior, market manipulation, malpractice, or other related financial industry laws or regulations	In accordance with applicable securities laws and regulations, ICE includes a description of material legal proceedings (including of the type, if any, described in FN-EX-510a.1) in our annual and quarterly filings on, respectively, Forms 10-K and 10-Q.
FN-EX-510a.2	Discussion of processes for identifying and assessing conflicts of interest	<p>ICE has adopted a <b>Global Code of Business Conduct</b> that applies to its employees, directors, consultants and contractors. The Global Code of Conduct clearly sets out the process by which conflicts of interest are identified, reported and managed. ICE conducts annual training for its employees on its Global Code of Business Conduct.</p> <p>ICE's Nominating and Corporate Governance Committee is responsible for devising and proposing to the Board of Directors a code of business conduct for directors, officers and employees addressing, at a minimum, conflicts of interest and compliance with applicable laws, rules and regulations, including compliance and enforcement mechanisms, and monitor compliance with such code of business conduct. The Nominating and Corporate Governance Committee reviews and approves, if deemed appropriate, all requests for waivers of the Global Code of Business Conduct.</p> <p>In addition, conflicts of interests would be identified and assessed through ICE's quarterly financial disclosure procedures and annual director and officer questionnaires.</p>
<b>Managing Business Continuity &amp; Technology Risks</b>		
FN-EX-550a.2	(1) Number of data breaches, (2) percentage involving personally identifiable information (PII), (3) number of customers affected	<p>(1) Number of data breaches - None</p> <p>(2) percentage involving personally identifiable information (PII) - NA</p> <p>(3) number of customers affected - NA</p>

<p>FN-EX-550a.3</p>	<p>Description of efforts to prevent technology errors, security breaches, and market disruptions</p>	<p>ICE ensures both the physical and digital security of our markets, clearing houses, data and mortgage software through industry-leading security technology and processes.</p> <p><b>Cybersecurity</b></p> <p>Our Information Security Department consists of diverse and skilled teams that work to protect confidential data and systems from unauthorized access, misuse, disclosure, destruction, modification or disruption.</p> <p><b>Policy and governance</b></p> <ul style="list-style-type: none"> <li>■ A formal cybersecurity strategy is maintained by management and approved by the Risk Committee.</li> <li>■ Detailed cybersecurity policies are reviewed at least annually.</li> <li>■ Board oversight is led by the Risk Committee with at least quarterly security briefings from senior management.</li> <li>■ Service Organization Control (SOC2, type II) assessments are performed annually to produce independent verification and testing of ICE controls for external parties and auditors that rely on ICE. The scope of these reports is evaluated each year and tailored in response to customer feedback and business developments. These reports are available to any customer via the Customer Third-Party Risk Management Portal.</li> <li>■ Periodic third-party assessments are conducted using the NIST Cybersecurity Framework to measure program maturity and completeness.</li> <li>■ We maintain insurance coverage that may, subject to the terms and conditions of the policy and payment of deductibles, cover certain aspects of cybersecurity issues.</li> <li>■ Reporting a security concern can be done easily from our website <a href="#">here</a>.</li> </ul> <p><b>Team</b></p> <ul style="list-style-type: none"> <li>■ The lead independent director of ICE's Board has expansive cybersecurity and risk expertise, including on the National Infrastructure Advisory Council (NIAC), a White House homeland defense initiative that protects information systems critical to the nation's infrastructure, where he served through 2020.</li> <li>■ A dedicated cybersecurity team is led by the Chief Information Security Officer, with specialized teams of subject matter expertise: <ul style="list-style-type: none"> <li>- Digital forensics and incident response</li> <li>- Red team</li> <li>- Threat intelligence and cyber fraud</li> <li>- System architecture and automation</li> <li>- Governance, risk and compliance</li> <li>- Application security</li> <li>- Cloud security</li> </ul> </li> <li>■ ICE has a dedicated threat intelligence team monitoring public and private sources of emerging threats and vulnerabilities, while also participating extensively in industry and government sponsored information-sharing groups to ensure awareness of ICE-specific and sector level threats.</li> <li>■ ICE requires ongoing training for Information Security staff to ensure fluency in their respective areas.</li> </ul> <p><b>Employee training</b></p> <ul style="list-style-type: none"> <li>■ Information security is considered a core skillset and is part of every employee's annual performance review.</li> <li>■ Employees are required to complete extensive security awareness training upon hire and annually thereafter; training modules require employees to read and provide acknowledgement of the Corporate Information Security Policy.</li> <li>■ Phish testing campaigns are conducted each quarter with all employees.</li> </ul>
---------------------	---	--

		<ul style="list-style-type: none"> <li>■ Information Security Assurance regularly conducts tests utilizing various methods to verify compliance with written policies and to assess vulnerabilities. In addition, ICE teams are subject to examinations from Enterprise Risk, Internal Audit, and multiple international regulatory bodies.</li> </ul> <p><b>System Resiliency and Business Continuity Planning / Disaster Recovery</b></p> <p>Our crisis management team handles our end-to-end response to any potential issues and regularly conducts global drills to ensure our processes are ready to be implemented. Our operations team maintains an incident management program to handle any incident with operational impact - security or otherwise. The goal of the incident management program is to provide a cohesive framework for the communication, resolution and recording of incidents and to ensure incidents are resolved in a planned and controlled manner so that any interruption is resolved quickly and normal operations are restored.</p> <ul style="list-style-type: none"> <li>■ System resiliency and business continuity management is a core tenant of our system design process and redundancies are purpose-built into our applications, network infrastructure and across primary and backup data centers.</li> <li>■ Such design resiliency may include “hot/hot” system components with real-time failure capabilities, readily available back-up components, robust recovery and/or failover procedures, and geographically-diverse backup data centers. These geographically-diverse “like for like” disaster recovery data centers are maintained and governed by an enterprise wide policy. Per policy, all ICE core procedures, systems and operational tasks are duplicable in recovery facilities, exercised at least annually and documented comprehensively.</li> <li>■ Following each acquisition of a new company, this process is reviewed to ensure crisis management procedures are in place across our entire organization.</li> <li>■ Board oversight includes quarterly reports to the Risk Committee on technology operations and governance.</li> <li>■ Employees are trained annually on our business continuity procedures to ensure readiness and understanding.</li> </ul>
--	--	---

**Environmental Footprint of Hardware Infrastructure**

TC-SI-130a.1	(1) Total energy consumed, (2) percentage grid electricity, (3) percentage renewable	We calculate and report our greenhouse gas emissions using the GHG Protocol including all Scope 1, Scope 2 and relevant 3 categories. This data can be found in our <b>annual sustainability report</b> as well as our <b>TCFD report</b> .
TC-SI-130a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	<p>We focus our energy management program on our two data centers, where we can make the most material difference. Our centers have implemented industry leading techniques to improve energy efficiency, reduce waste and offset operating emissions. The building structures provide a high level of insulation to minimize outside air infiltration and reduce solar heat gains. This lowers the thermal losses of the building which delivers a more efficient cooling profile and reduces the energy demand.</p> <p>The most commonly used and cited metric for data center energy efficiency is Power Usage Effectiveness (PUE). At our data centers, we have consistently delivered a PUE that has outperformed the base building design by up to 14% by implementing multiple mitigation tactics including: optimized thermal stratification, data center air management, high efficiency HVAC chillers, speed control on cooling equipment and automated lighting control systems.</p> <p>Our Basildon data center was built to stringent specifications allowing us to attain the following ISO accreditations:  ISO 9001  ISO 14001  BSEN 18001  ISO 50001</p>

<b>Data Privacy &amp; Freedom of Expression</b>		
TC-SI-220a.1	Description of policies and practices relating to behavioral advertising and user privacy	Users of ICE websites, applications and services have full informed control over tracking preferences. Analytics cookies may be used on some ICE web addresses to track user traffic across web properties. Individuals who browse ICE websites have full control over their cookie preferences and give their affirmative informed consent to the use of any cookies that are not strictly necessary for website functionality.
TC-SI-220a.2	Number of users whose information is used for secondary purposes	None. ICE uses personal information only for the specific purposes authorized.
TC-SI-220a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	In accordance with applicable securities laws and regulations, ICE includes a description of material legal proceedings (including of the type, if any, described in TC-SI-220a.3) in our annual and quarterly filings on, respectively, Forms 10-K and 10-Q.
TC-SI-220a.4	(1) Number of law enforcement requests for user information, (2) number of users whose information was requested, (3) percentage resulting in disclosure	ICE has received no requests for user information under the Foreign Intelligence Surveillance Act (FISA). ICE has received requests to provide user information pursuant to a criminal warrant less than five times and provided the information in each instance.
TC-SI-220a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	None.
<b>Data Security</b>		
TC-SI-230a.1	(1) Number of data breaches (2) percentage involving personally identifiable information (PII) (3) number of users affected	(1) None (2) NA (3) NA
TC-SI-230a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	See FN-EX-550a.3
<b>Recruiting &amp; Managing a Global, Diverse &amp; Skilled Workforce</b>		
TC-SI-330a.1	Percentage of employees that are (1) foreign nationals and (2) located offshore	(1) 8% of our employees are on a Visa (2) 42% of our employees are based outside the United States
TC-SI-330a.2	Employee engagement as a percentage	We measure employee engagement in a number of ways including through the following question on our biennial employee survey: "Overall, I would recommend ICE to a friend as a good place to work." 85% of our employees agreed or strongly agreed with this statement in our most recent employee survey.
TC-SI-330a.3	Percentage of gender and racial/ethnic group representation for (1) management, (2) technical staff, and (3) all other employees	We report gender and diversity metrics for our US and UK employee populations, including our EEO-1 report. We are focused on increasing diversity throughout our organization and broader community including at the board and senior management team levels as well as throughout our ranks. Our strategy and efforts are outlined in our annual sustainability report and on our website.  <b>Diversity data</b> → <b>Diversity strategy</b> →
<b>Intellectual Property Protection &amp; Competitive Behavior</b>		
TC-SI-520a.1	Total amount of monetary losses as a result of legal proceedings associated with anticompetitive behavior regulations	In accordance with applicable securities laws and regulations, ICE includes a description of material legal proceedings (including of the type, if any, described in TC-SI-520a.1) in our annual and quarterly filings on, respectively, Forms 10-K and 10-Q.
<b>Managing Systemic Risks from Technology Disruptions</b>		
TC-SI-550a.2	Description of business continuity risks related to disruptions of operations	We disclose risk factors in our Form 10-K including those related to operations.

## Table 2. Activity Metrics

Code	Metric	2021 Performance
FN-EX-000.A	Average daily number of trades executed, by product or asset class	We report trading volumes monthly across our exchanges and asset classes <a href="#">here</a> and daily volumes <a href="#">here</a> .
FN-EX-000.B	Average daily volume traded, by product or asset class	We report trading volumes monthly across our exchanges and asset classes <a href="#">here</a> and daily volumes <a href="#">here</a> .

Metrics included for the Security & Commodity Exchanges and Software & IT Services sectors where relevant for our business.