Industry Classification Methodology Guide

ISE Cyber Security® Industry Classification

Table of Contents

Chapter 1. Introduction

Given the lack of an existing generally accepted equity classification scheme identifying and cataloging equity securities of companies involved in the cyber security industry, the **ISE Cyber Security® Industry Classification** was developed by ISE. The **ISE Cyber Security® Industry Classification** provides a framework for investment research, portfolio management and asset allocation. Eligible companies are publicly listed on exchanges globally and derive all or a "material" proportion of their revenues from cyber security or cyber security-related activities.

ISE is responsible for the classification of companies within the **ISE Cyber Security® Industry Classification**, maintenance of the database of companies comprising the **ISE Cyber Security® Industry Classification**, including the history of changes, and the timely communication of any updates to licensees of the data.

Chapter 2. Industry Classification

2.1. Structure and Changes

The Classification Committee will rely primarily on published audited annual reports and discussions with company investor relations groups, industry participants and experts to vet companies for inclusion and determine their classification. Companies are allocated into a category based on the focus of their business. In cases where a company's business straddles two or more segments, a final category determination will be made based on audited reported revenue segments as well as discussions with that company's investor relations group.

Qualified and newly listed companies are assessed and approved by the Classification Committee for inclusion in the **ISE Cyber Security® Industry Classification**.

As the cyber security industry continues to evolve, the framework of the **ISE Cyber Security® Industry Classification** will evolve in order to accurately reflect the then-current state of the cyber security industry. Any adjustments to the framework of the **ISE Cyber Security® Industry Classification** will be based on long-term trends driving the cyber security industry and will be announced in advance of implementation.

In the event of a significant change to a company's structure or business, its classification may be reviewed on an ad hoc basis. Events triggering a review include, but are not limited to: mergers, acquisitions, bankruptcy and delisting. Companies will also undergo a quarterly review.

Companies may not apply, and may not be nominated for inclusion in the **ISE Cyber Security® Industry Classification**.

Additions and deletions to the list of companies eligible for classification may occur on an ad hoc basis and is dependent wholly on the reported activities of those companies.

No changes in the **ISE Cyber Security Index Classification** will be based on non-public information.

2.2. Classification Guidelines

All equities listed on exchanges globally are eligible for review. Companies are classified quantitatively and qualitatively. Each company is assigned to a single category according to its principal business activity based on audited financial reporting including the director's report. ISE uses revenues as a key factor in determining a company's principal business activity. Earnings and market perception are also recognized as important and relevant information for categorization purposes and are taken into account during the review process.

The scope of the definition of cyber security can be quite broad. For the purposes of the **ISE Cyber Security Index Classification**, we consider cyber security to be concerned with enabling the protection of and secure communication between unique nodes of the internet from both external and internal threats.

The basic eligibility determinant for inclusion in the **ISE Cyber Security Index Classification** is that prospective companies are either those which work to develop hardware and/or software that safeguards access to files, websites and networks from external origins or those that utilize these tools to provide consulting and/or secure cyber based services to their clients.

These two categorizations have been labeled as:

i) **Infrastructure Provider** – a company that is a direct provider of hardware or software for cyber security and for which cyber security business activities are the key driver of the business or,

ii) **Service Provider** – a company whose business model is defined by its role in providing secure cyber based services and for which those business activities are a key driver of the business.

2.3. Infrastructure Provider

These companies provide hardware and/or software that help route and regulate message traffic in and out of networks.

Anti-Virus - Companies providing anti-virus solutions fall into the definition of Infrastructure Provider as they provide protection against threats originating from external sources.

Network Security - Examples of the type of network hardware products these companies produce include gateways, routers, bridges and switches. The set of operating instructions and security, referred to as a firewall, is usually bundled with the specific hardware element by the manufacturer although third party software can often be adapted to work outside of its native environment. In the case of firewalls, often times, third-party solutions can provide more robust solutions than those packaged with network hardware.

2.4. Service Provider

These companies provide services that fall outside the narrow definition of Infrastructure Provider. Service Providers allow for their clients to conduct business securely while Infrastructure Providers are providing security itself. For example, a company may be engaged in domain name management or managing the efficient routing of internet traffic but do not have the responsibility for the security of the domains themselves or the nature of the traffic they are routing. Another example would be companies involved in the manufacture of secure credit cards, network authentication devices and/or electronic identity documents.

Chapter 3. Classification Committee

The Classification Committee is comprised of employees of Nasdaq. Additional resources include direct contact with companies engaged in cyber security and industry associations supporting the cyber security industry.

The Classification Committee will meet on a quarterly basis to discuss any proposed changes to the **ISE Cyber Security® Industry Classification**.

Ad hoc meetings may be convened at the discretion of the Classification Committee.

Meetings will typically consist of discussion and review of the framework and company classifications to ensure that the **ISE Cyber Security® Industry Classification** continues to reflect the then-current state of the cyber security industry.