FINRA Compliance IT Checklist

As a regulatory organization that oversees and regulates broker-dealers in the United States, FINRA institutes regulations and guidelines related to technology to ensure your firm is implementing technology in a responsible and compliant manner. These guidelines include cybersecurity, data protection, business continuity planning, electronic communications, social media, algorithmic trading, outsourcing, cloud computing, third-party vendors, and supervision.

You must have appropriate controls and procedures in place to ensure compliance with these regulations and guidelines. It is critical for your firm to stay up-to-date on FINRA's technology-related regulations and guidelines. 911 IT is the answer to this challenge. We have experience navigating this space and are an invaluable help to your firm as you reach and maintain compliance. Learn more.

FINRA (Financial Industry Regulatory Authority) is a regulatory organization that oversees and regulates the activities of all broker-dealers in the United States. As technology keeps changing and plays an increasingly important role in the financial industry, FINRA has introduced regulations and guidelines to ensure that firms are implementing technology in a responsible and compliant manner. Here are key terms and a checklist of the technology-related requirements that FINRA has introduced:

Terms

Access Control
The process of limiting access to computer systems, networks, and data to authorized users only. Access control includes the use of passwords, encryption, firewalls, and other security mechanisms.

Authentication
The process of verifying the identity of a user, device, or system. Authentication can be done using a password, biometric data, or a security token.

Authorization
The process of granting or denying access to a user, device, or system based on their identity and the permissions they have been granted.

Data Loss Prevention (DLP)
The process of identifying, monitoring, and protecting sensitive data to prevent its unauthorized disclosure or theft.

Encryption
The process of converting data into a form that can only be read by someone who has the encryption key. Encryption is used to protect data in transit and at rest.

Firewall
A security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.

Incident Response
The process of detecting, investigating, and responding to security incidents. The incident response includes steps such as containment, eradication, and recovery.

Intrusion Detection System (IDS)
A system that monitors network traffic for signs of unauthorized access or malicious activity.

Malware
Any software designed to harm or exploit computer systems, networks, or data. Malware includes viruses, worms, trojans, and other malicious software.

Penetration Testing
The process of simulating a cyberattack to identify vulnerabilities in a system or network.

Phishing
A type of social engineering attack that uses email, phone calls, or other means to trick users into divulging sensitive information or performing actions that compromise security.

Risk Assessment
The process of identifying, analyzing, and evaluating the potential risks to an organization's assets, systems, and data.

Social Engineering
The use of deception to manipulate individuals into divulging sensitive information or performing actions that compromise security.

Vulnerability Assessment
The process of identifying, analyzing, and evaluating the vulnerabilities in a system or network.

FINRA Security Checklist

Cybersecurity
Firms must have a comprehensive cybersecurity program in place that includes regular risk assessments, employee training, and incident response plans.

Data protection
Firms must protect sensitive customer information and ensure that it is stored securely.

Business continuity planning
Firms must have plans in place to ensure that they can continue to operate in the event of a disaster or other business interruption.

Electronic communications
Firms must ensure that all electronic communications with customers are captured and stored in accordance with regulatory requirements.

Social media
Firms must have policies in place governing the use of social media by employees and ensure that all social media activity is captured and stored.

Algorithmic trading
Firms that use algorithmic trading strategies must implement controls to ensure that the algorithms are functioning as intended and do not pose a risk to market stability.

Outsourcing
Firms that outsource technology functions must have policies and procedures in place to ensure that the outsourced functions are being performed in a compliant manner.

Cloud computing
Firms that use cloud computing services must ensure that the services are being used in a compliant manner and that appropriate security controls are in place.

Third-party vendors
Firms that use third-party vendors for technology-related services must conduct due diligence to ensure that the vendors are capable of performing the services in a compliant manner.

Supervision
Firms must ensure that they have appropriate supervisory procedures in place to monitor their technology-related activities and ensure compliance with regulatory requirements.

Resources:

FINRA Compliance Tools - Cybersecurity Checklist
National Institute of Standards and Technology (NIST) Cybersecurity Framework
FINRA's Report on Cybersecurity Practices