CYBER SECURITY STANDARDS IN FINANCIAL INDUSTRY

An organisation might employ a collection of rules or best practises known as a cybersecurity standard to strengthen its cybersecurity posture. Cybersecurity standards may be used by businesses to help them identify and put in place the right defences against online threats to their systems and data. Additionally, standards can offer direction on how to handle and recover from cybersecurity events. No matter the size, industry, or sector of the organisation, cybersecurity guidelines are typically relevant.

There are several global and local cybersecurity standards that are used in the Financial Sector.

Global Cyber Security Standards:

- PCI DSS (Payment Card Industry Data Security Standard):

It outlines the conditions for the handling, processing, and transmission of payment card information. The standard aims to lessen instances of credit card fraud and enhance cardholder data security.

- ISO/IEC 27001 (International Organization for Standardization/ International Electrotechnical Commission):

This standard specifies guidelines and suitable practises for handling security concerns, particularly handling financial data.

- SWIFT CSP (SWIFT Customer Security Programme):

This framework outlines specifications for appropriately managing access, safeguarding data, and handling incidents.

In addition to the global compliances there are some local guidelines as well that vary from region to region. Some of the most well known and common are:

- SOX (Sarbanes Oxley Act):

  It suggested methods that businesses might use to avoid processing fraudulent money transactions. It details, in particular, what financial records must be kept, for how long, and how they must be safeguarded.

- GLBA (Gramm-Leach-Bliley Act):

It suggested methods that businesses might use to avoid processing fraudulent money transactions. It details, in particular, what financial records must be kept, for how long, and how they must be safeguarded.

- FINRA (Financial Industry Regulatory Authority):

Having documented data protection rules is essential for preventing the compromise of customer data, among other things. Additionally, FINRA provides guidelines for identifying and minimising online dangers.

- PSD 2(Payment Services Directive):

This establishes stringent guidelines for the security of consumers' private data and specifies regulations for how electronic payments must be started and processed.

- BSA (Bank Secrecy Act):

This deters and alerts authorities to tax evasion, money laundering, and the financing of terrorism.

- NIST(National Institute of Standards and Technology):

It suggests risk management for cybersecurity, data security, threat detection, and incident handling.

- GDPR(General Data Protection Regulation):

It is a framework for data privacy that establishes guidelines for gathering, keeping, transferring, and processing the personal information of EU citizens.