IT Security & Compliance Management

Many of the following are MANDATORY

GDPR (General Data Protection Regulation) Compliance

- GDPR has only been passed in Europe but it affects the world.
    - One of the primary goals of the GDPR is to give personal data back to citizens and residents of the EU. This is reflected by requirements that subjects give consent before data is processed, that collected data is anonymized and safely handled when transferred and breches are handled with urgency and care.

Who Does GDPR Apply To?

As an EU regulation, GDPR is designed to protect the personal data of data subjects residing in the EU. Specifically, Article 3 of the GDPR states that it applies to the processing of personal data of citizens and residents of the EU, even if the processor isn't established in the EU. Practically, this Article of the GDPR means that these Regulations apply to any company marketing goods or services to EU residents and citizens. These include:

- **European States:** Government entities that handle the personal data of citizens and residents of the EU are as much subject to GDPR rules as any company.
- **European Companies:** EU companies, since they are both located within the EU and handle transactional and personal data of EU citizens and residents, are expected to comply with GDPR.
- **Global Companies:** Any company that markets goods and services to EU states and completes transactions with EU citizens and residents are also expected to maintain GDPR compliance, regardless of where the corporation is located. Even if they have no staff or equipment located in the EU, if their marketing efforts extend to the EU or they use personal data to track the behavior of EU citizens, they are subject to GDPR rule
    - Because of the world's increasingly global economy, more companies than ever are working in the EU, marketing and selling to EU citizens. From app developers to Internet-based businesses and multinational corporations, businesses worldwide work with EU citizens and residents. This means that the types of companies subject to GDPR laws are so varied and widespread that the implementation of GDPR will have a global effect on data protection requirements. This is yet another difference between the GDPR and the 1995 Directive, as the Directive was not nearly as expansive or far-reaching.

IT Security & Compliance Management

Many of the following are MANDATORY

HIPAA (Health Insurance Portability and Accountability Act) compliance

- HIPAA is a set of regulations concerning the handling of medical information, including privacy and security. The regulation requires that any companies handling healthcare data, from hospitals to insurance companies, must comply with HIPAA security standards when transmitting and storing electronic protected health information (ePHI).

Why is Compliance With HIPAA Important?

- Compliance with HIPAA standards is required of all healthcare businesses due to the sensitive nature of information handled by these companies. A single cyber attack on a health-related business can result in lost or stolen data that has broad ramifications on the health, safety and financial security of patients, and these attacks are becoming both more frequent and more aggressive. Failing to comply with HIPAA standards can result in severe consequences for healthcare businesses, including:
    - **Reputational:** The moment it's revealed that a company's information was hacked, that company's reputation decreases. This is particularly true for healthcare businesses due to the sensitive nature of the information they carry. Such reputational damage can negatively impact future business and lose the trust of patients and partners alike.
    - **Legal:** Since HIPAA compliance is a federal requirement of all healthcare businesses, failure to comply with HIPAA requirements can result in severe fines. These fines multiply if a breach occurs as a result of HIPAA noncompliance. Patients may even sue the business because of their negligence.
    - **Financial:** Between the reputational and legal damage done to a healthcare organization due to HIPAA noncompliance, financial damages can be steep. Often, these damages are enough to bankrupt entire healthcare enterprises.
        - These factors mean HIPAA compliance is an absolute must. While these regulations won't protect against all threats your healthcare business might face, they pose a strong baseline off of which your business can build. The first step, however, is to achieve HIPAA compliance.

IT Security & Compliance Management

Many of the following are MANDATORY

Sabranes-Oxley Act (SOX) Compliance

- Complying with the Sarbanes-Oxley Act involves maintaining financial records for seven years and is required for U.S. company boards, management personnel and accounting firms. The point of the regulation was to prevent another incident like the Enron scandal, which hinged on fraudulent bookkeeping.
    - SOX was designed with the goal of implementing accounting and disclosure requirements that:
    - Increase transparency in corporate governance and financial reporting
    - Formalize a system of internal checks and balances
        - SOX is applicable to:
        - All publicly held American companies
        - Any international companies that have registered equity or debt securities with the U.S. Securities and Exchange Commission (SEC)
        - Any accounting firm or other third party that provides financial services to either of the above
        - Penalties for non-compliance: Formal penalties for non-compliance with SOX can include fines, removal from listings on public stock exchanges and invalidation of D&O insurance policies. Under the Act, CEOs and CFOs who willfully submit an incorrect certification to a SOX compliance audit can face fines of $5 million and up to 20 years in jail.

IT Security & Compliance Management

Many of the following are MANDATORY

FISMA (Federal Information Security Management) Compliance

- The Federal Information Security Management Act of 2002 treats information security as a matter of national security for federal agencies. As part of the bill, all federal agencies are required to develop data protection methods.
    - FISMA, or the Federal Information Security Management Act, is a piece of United States legislation that defines a framework designed to protect government information, operations and assets from threats. The legislation does this by assigning responsibilities to various agencies and groups to ensure data security from both human-made and natural disasters.
        - It also requires contractors to take certain steps toward tighter data security. Failure to follow these regulations can result both in breaches and censure from the United States government, along with reduced federal funding.

IT Security & Compliance Management

Many of the following are MANDATORY

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

- PCI - DSS is a set of regulations meant to help reduce fraud, primarily through protecting customer credit card information. PCI-DSS security and compliance is required for all companies handling credit card information.

What is PCI-DSS?

- The Payment Card Industry Data Security Standard, more commonly known by its acronym, PCI DSS, is a globally recognized set of guidelines. Put in place by the Payment Card Industry Security Standards Council, or PCI SSC, this standard is a requirement for the majority of businesses today, as most handle or interact with credit card data and other sensitive customer information.
    - PCI DSS compliance primarily entails maintaining a secure data network, regularly monitoring networks and implementing security controls, among other rules. Though these rules may seem simple, they can be difficult to maintain in combination with other security measures. However, failure to comply can result in steep penalties and fines. In short, PCI DSS compliance is essential for any organization handling credit card information.