How Does Regulatory Compliance Affect the Software Development Process?

Digital Transformation projects can impact virtually every aspect of a business, its employees and its processes and operations. But regulatory compliance is one area that many fail to consider, leading to some potentially serious and very costly risk management issues.

Let's take the example of business messaging. Perhaps you have a stand alone messaging app for your company. Or maybe you opted to include a messaging feature as part of a larger enterprise software platform. It's been months since your company started using these messaging tools and suddenly, you're confronted with massive fines and penalties because your messaging platform fails to comply with regulations or even recordkeeping laws.

That's exactly what happened to nearly a dozen well-known banks, including Goldman Sachs, Morgan Stanley, Bank of America, Citigroup, Cantor Fitzgerald & Co, UBS Group, Deutsche Bank and Barclays. Collectively, they were fined nearly $2 billion dollars by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC).

The bank employees were found to be using consumer-grade messaging apps to communicate with clients, but these platforms

lacked the tools required to be compliant with recordkeeping laws. As consumer-grade messaging apps, they lacked data retention capabilities and data export tools, amongst other things. The end result: an inability to comply with recordkeeping laws. And while these cases involved consumer-grade messaging platforms, an in-built messaging feature included as part of a Digital Transformation project could easily lead to a similar situation involving regulatory non-compliance. This underscores the importance of understanding exactly how regulatory compliance affects the software development process.

Understanding Your Regulatory Compliance Landscape

To achieve and maintain compliance, you'll need to achieve a solid understanding of your regulatory compliance burdens. Highly-regulated industries such as the medical and health care fields or the financial sector are usually very aware of their regulatory compliance burdens. Many address regulatory compliance rather extensively as part of their risk management efforts. But less heavily regulated companies may fail to consider compliance as they go through the Digital Transformation development process. For this reason, it is important to take some time to understand what your business needs to do in order to achieve and maintain regulatory compliance in your software platform, mobile app or other Digital Transformation project.

Key areas of consideration typically surround data and may include the following.

- **Data collection** - What data are you collecting? How is that data collected?
- **Data storage** - Where and how is data stored? Is that data encrypted and protected?
- **Data retention** - What data do you need to retain? What's the minimum retention timeframe?
- **Data access** - Who is allowed to access specific types of data? How is data access managed?
- **Data transmission** - How is data transmitted from collection point to the data storage site? Are there protections in place such as encryption?
- **Data protection** - How is data protected when it's being transmitted and stored? Are you using end-to-end encryption? How are data breaches detected and handled?

These are just a few of the questions that will need to be considered as you proceed with the software development process. But when all is said and done, it is much easier to address regulatory compliance when you're at the start of a Digital Transformation project. Addressing challenges down the road and scrambling to correct a compliance-related issue is virtually always going to be more difficult and more costly.

While regulatory compliance is largely industry specific, there are lots of more general, far-reaching regulations that must be

considered. One example is GDPR, which governs data handling for all companies and websites that deal with EU citizens. GDPR fines can be significant too, reaching up to 10 million euros or up to 2% of the company's worldwide turnover for the prior year — whichever figure happens to be highest.

Planning for Regulatory Compliance During the Software Development Process

Once you've identified your regulatory compliance burdens, you will need to ensure that your mobile app or software platform allows for full compliance. Each feature and functionality must be considered relative to your company's compliance requirements — a high-stakes task that's much easier said than done.

Regulatory compliance is a key issue that must be addressed as you develop your software and business requirements documents. By taking a proactive and intentional stance on regulatory compliance, your company will be well-positioned to move forward with confidence knowing that you won't be facing massive fines and penalties down the road.

Many larger companies may have a risk management team that can provide valuable insights when it comes to the issue of regulatory compliance. For this reason, it can be beneficial to include these risk management team members in the software

development process since they can offer useful insights that may otherwise go unrealized.

(Company-specific conclusion and call-to-action redacted.)