How to Conduct a Compliance Risk Assessment

The privacy landscape has changed significantly since GDPR went into effect in 2018. In fact, Gartner predicts that by 2023, privacy regulations will cover personal data of 65 percent of the global population. These regulations place a heavy responsibility on the organizations that hold the data. Conducting a regular compliance risk assessment, therefore, proves essential.

The National Institute of Standards and Technology (NIST) defines privacy risk assessment as "a process that helps organizations to analyze and assess privacy risks for individuals arising from the processing of their data."

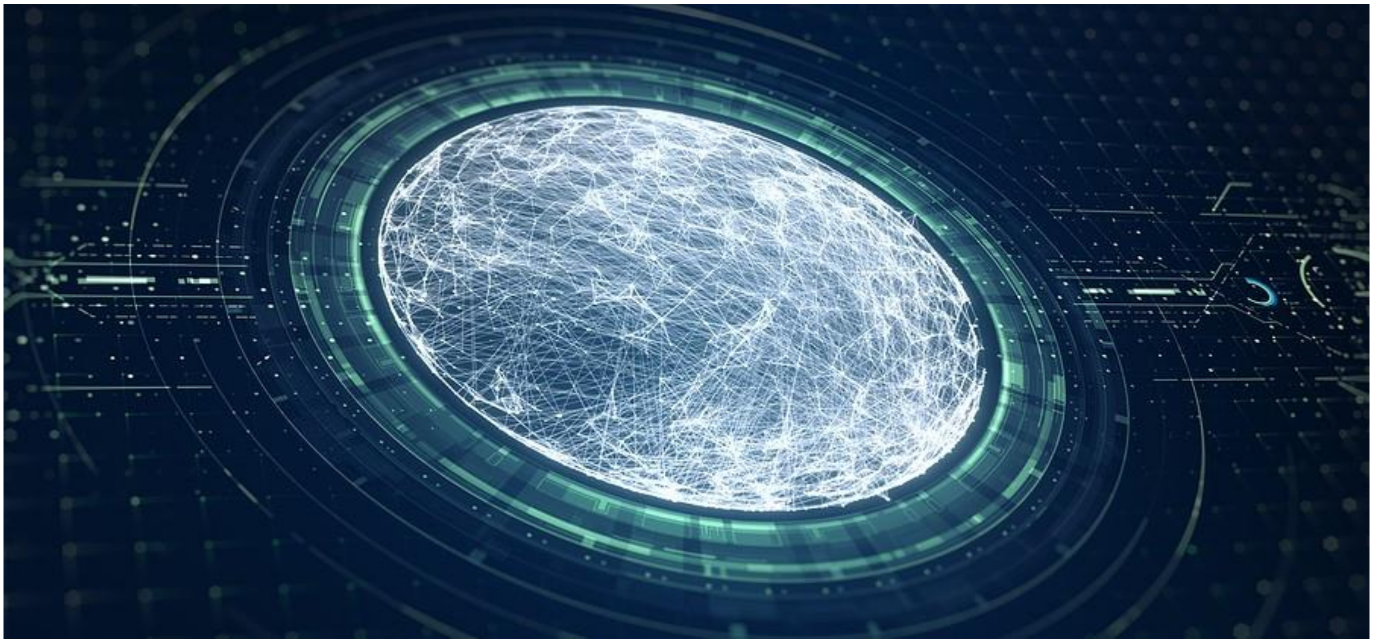
From a data perspective, this means that organizations must first determine what the existing rules and regulations require of them. Then, they need to evaluate whether organizational policies and processes fulfill those requirements. While individual assessments will vary in the details, a few basic steps apply to almost any risk assessment.

1. Assess the Data Compliance Landscape

To determine the current compliance landscape, the organization must first answer the question of where they do business. This applies to both geographical location and industry and extends beyond the location of the home office. For instance, a business in Oregon may market through their website to customers across the country.

Second, the organization needs to determine what privacy regulations apply. This includes location-based regulations like GDPR and CCPA. It also includes industry-specific laws, such as HIPAA for healthcare organizations. Additionally, the assessment should address internal policies or contractual obligations related to data privacy.

Keep in mind that as organizations evolve, changes occur that affect the compliance landscape. For instance, marketing to a new geographical location or acquiring another company may introduce new regulatory controls. Likewise, the regulations themselves evolve, and additional laws come into effect every year.



2. Understand Data Flow

With an understanding of the compliance landscape, you can then assess data flow. This involves knowing what data the company holds, where it lives, and what policies and procedures affect the data. For instance, does the organization have retention policies in place? What security measures exist to protect sensitive data in transit and in storage?

As you analyze the data flow, be sure to address all avenues involved in collecting, using, and sharing information. For instance, client-facing websites present unique vulnerabilities as they collect data from customers. Likewise, identify all third parties that have access to sensitive data and what controls exist in those arenas. A strong data governance program helps this process.

3. Analyze and Evaluate Risks

Now that you know what regulations apply and have a picture of the data flow and policies within the organization, you can identify and prioritize risks. Your goal in this step is to accurately identify whether the organization can meet regulatory requirements. Even if the answer is "no," it gives you a place to start.

No organization will have zero risk. However, by mapping regulatory requirements to existing data controls and procedures, you will identify weak points and prioritize an approach. Through this analysis process, you can determine the level of risk and identify areas of focus.

This involves determining the likelihood that a given threat will occur, along with the severity of the impact. If the threat could have a major impact, but the likelihood of it occurring is rare, the risk level probably remains low. On the other hand, if the threat could deliver major impact and is likely to occur, the company must take action.

4. Document and Implement Findings

Armed with identified risks, administrators develop and implement a plan to improve the company's compliance posture. Focus on high-risk areas. Additionally, keep in mind the balance between too rigid compliance that halts productivity and overly lax compliance that results in stiff penalties.

Develop a Compliance Risk Assessment Tailored to Your Needs

The compliance risk assessment provides several key benefits in addition to avoiding penalties. For instance, it shows customers, investors and the public that the organization values and protects privacy. It also helps to uncover potential issues before they become problems, saving time and money. And it guides strategic decision making.

Compliance monitoring and privacy risk assessments can prove complicated. But the data consultants at Messaging Architects will help your organization implement proactive data governance. Combining data management best practices with compliance monitoring and multilevel data security will protect both you and your customers.