Haekka

Lesson 2 | Security vs Privacy vs Compliance

Updated 2020-09-14

The differences between the terms of *privacy*, *compliance*, and *security* are rarely appreciated. While the words are related, they are separate and distinct functions. For smaller companies, these functions often overlap with employees having ownership and accountability across two or even all of these domains. As organizations grow, there is more separation between the functions and entire departments dedicated to each one.

Below is a summary table of how the functions are different from each other. These are very general rules that can differ from company to company.

Function	Work Streams	Deliverables	Budget
Privacy	- Privacy official - Privacy policies - Privacy training	- Policies and procedures - Few tools	$
Security	- Implementations - Security ops - Security training	- IT security procedures - Many tools	$$$$$
Compliance	- Risk- Audit - Internal and external - Regulatory mapping	- Audit reports - Risk management - GRC	$$

In practicality, the functions need to work together to create a functional privacy stack called an information security management system (ISMS), compliance program, or privacy program.

Each of the functions builds on the others. Privacy defines the policies and procedures for the ways data should be handled and protected. Security implements controls and technology to meet the policies and procedures. And compliance verifies the chain from privacy up through security does not have gaps.

Privacy makes promises -> Security implements those promises -> Compliance validates promises.

Ideally, these functions have boundaries to ensure the separation of duties and to avoid conflicts of interest.

The following sections go into more detailed explanations of each function.

Privacy

Privacy is the first step. Once a compliance DNA, or framework, is chosen or assigned to an organization, relevant regulatory controls are addressed with privacy policies and procedures. Given the dynamic nature of compliance regulations in 2020, privacy policies and procedures need to be revisited and kept up to date.

Security

Once privacy policies have been written and acknowledged by all employees, it is up to security to implement them. Security often falls under IT. Security is in charge of configurations and security monitoring, with a plethora of new tools in the market and lots of noise from constant alerts.

With rapidly changing technology, especially services from cloud providers like AWS, Google, and Microsoft, keeping security configurations up to date is a constant challenge.

Compliance

Compliance is about keeping promises. It's about building trust. It is the best representation to the market, customers, and partners that you have created and executed privacy policies and procedures. Compliance is mainly about proof, and the collection of that proof can be a bane on both security and privacy.

Compliance, in larger organizations, is lumped into Governance, Risk, and Compliance (GRC). GRC, both the functional area and the product category, is associated with large, enterprise companies. In smaller organizations, formal GRC groups rarely exist; in these smaller companies, the functions of governance, risk, and compliance are divided between ops, IT, legal, and HR.

In modern technology companies, even larger ones, SaaS tools accomplish the functions of GRC platforms. One notable example of this is Atlassian, which uses its software products for GRC.

Compliance, security, and compliance are separate and distinct functions that sometimes get lumped together at smaller organizations.