# A Crash Course in the Future of Cybersecurity and Compliance

## The Changing Landscape of IT Security

IT Security, cybersecurity, cyberwarfare; the names will evolve but the principles remain immutable. It is arguably one of the most provocative issue of modern times. It represents a point in our evolution that will occur only once, and has the potential for the most profound impacts on generations to come. I am speaking of what is today referred to as “digital transformation” (but has gone by many names). This is a bold statement in contrast to things like global warming, war, and so forth, but often it is the things that are not so obvious now that have the greatest impact on our future. Before we make a case for this essay we will begin with some basic concepts. It all starts with the fundamental principles of IT security, which is really a function of risk management, but let’s take one step at a time.

## What is Confidentiality, Integrity, and Availability

Simply put, when you boil it all down, these are the three categories of concern. Confidentiality, Integrity, and Availability are the pillars of IT security, and are values used to express and measure security compliance. The acronym is often referred to as the CIA triad, and represents, in most schools of thought, to be the core principles on which all information security is based.

Let’s break these principles down to better understand how they are applied in the course of information security practices. While common sense can go a long way to interpreting the importance and scope of these categories, their importance relative to each other will become more clear as we dive deeper. First, Confidentiality covers all the aspects of privacy and authentication, Availability covers our ability to access (or have access to) a system, and Integrity relates to how the data is maintained and safeguarded against adulteration. These principles are assessed within a system to determine the impact that would occur if one of these values is violated. A system is then rated with a low, medium, or high impact for each of these principles. A low impact means not much could happen if the principle is violated, but a high impact means bad things can happen. A systems overall security “impact rating” is based on the highest “watermark” of any one of these principles. In other words, if the Integrity impact is high (meaning bad things will happen if the data is not accurate), but the other two principles are low, the overall system watermark is still high (meaning a high impact or risk). This kind of assessment is known a Categorization and determines the “control measures” that will be “performed” to protect a system. As you can probably see in this abstract sense, the lines between risk management and information security are nonexistent when assessing impact.

Categorization is only the beginning, once you determine the things you are going to do, in other words the control measures you are going to apply, you must measure their success and adjust them as needed to be as cost effective as possible. This process of “tailoring” your control measures goes on forever, and is your “lifecycle”. At this point, IT security and risk management are one in the same.

## What is Compliance

So, what is compliance really? When we talk about compliance, we refer to the ability to show evidence that you have followed a process to identify and reduce risk, that you can prove you have established some sort of process rather than ad hoc “half measures” to alleviate an immediate threat. You may be doing the right things, but are you documenting why you are doing it? When it comes to compliance, the core principle is the continued practice of “tailoring” the scope of your practice through continuous performance of basic risk management principles. This means a continuous and ongoing process that can be reported on. In some cases, this is simple a spreadsheet with a list of concerns and what to do about them. Today, Managed Services have democratized the entire lifecycle so companies can simply subscribe to a risk management service for dollars a day and repurpose salaried positions accordingly. This is an interesting concept as most view risk management as a downsizing force, when in fact risk management focuses on efficiency and purpose. When applied correctly, positions are often adjusted to accommodate growth, but are rarely removed to improve the bottom line. With that said, it is the integrity of the data we use that influences the decisions we make.

## Why Is Integrity Becoming More Important?

In our current landscape, most risk comes from “bad actors” trying to circumvent authentication to gain access to data and monetize it. This is currently very profitable in the short term. However, a longer-term play is to modify the data in place or at rest in order to achieve a larger objective or subvert the data to your benefit. Unfortunately, this is happening all around us all the time. Let’s look at Wikipedia as an easy to understand example of what we are talking about. In terms of data integrity Wikipedia has established a control measure that requires several people to verify accuracy before information can be “verifiable”. The control measure can be easily thwarted however as many old timers know, if enough people collaborate the information can be completely adulterated, or as opinions change over time information is distorted. Research shows that information and sources tend to merge over time and become homogenized. In the past, we relied on books and ledgers, and origin, to ensure information was not adulterated, but that is no longer the case. Let’s look at another example; how many of us have had an erroneous charge on a bill and had some customer service representative explain that the computer is telling them that you owe them money when you know you don’t? In the old days, there were requirements for companies to prove the veracity of their billing data, but today those controls do not work in the consumers favor. If a company says you owe them money, you owe them money, period. It can be reported on your credit report and you can be put into collections. It is for this very reason that cyber criminals are flourishing, because protecting data integrity is very hard as it turns out.

## Where are we at now

We are ata point where The good news is that technology is starting to catch up with .

## The Next Big Thing

Managed Services allow consumers to focus on their core competency.