SteelCloud

Cybersecurity Risk vs. Compliance:

What is the Difference and Why It Matters

by Karl Walinskas, SteelCloud Business Development

Cybersecurity for computer networks and systems just keeps getting tougher every day, doesn't it? New attack vectors and threats occur by the hundreds on a daily basis. And those whose job it is to protect enterprise infrastructure know that the problem is bigger and more complex than the well-publicized major corporate and government breaches we hear about in the news that leave us concerned for our own cyber exposure as organizations and individuals. The threat is non-discriminant—not caring if we're a federal agency, corporation, small business, or an individual working from home. Cyber incursions are happening at scale, bad actors are behind them, and we have to eliminate or mitigate the risk.

Protecting systems and data requires massive defensive vigilance and action on the part of CISOs, CTOs, CIOs and the personnel that work for them at multiple points in the value chain of serving up information systems services to a needy customer base. This ranges from complying to standard requirements to continuous monitoring to changing attack surfaces using practices like Software Defined Networking (SDN) and all points in between. It has become conventional wisdom that the number of threats is too numerous to absolutely defend and defeat at 100% effect, so we hear terms like monitor, detect, contain, quarantine, remediate, and, sometimes, counter—all of which stem from the basic assumption that the bad guys are in, so what do we do about it?

But first, WHAT IS RISK?

Information Systems Security Officers (ISSOs) realize the overwhelming challenges of risk and compliance. They look to manage risk effectively to control the threat and prevent or mitigate bad outcomes but, "what exactly is risk?" Webster defines risk as exposure to possible loss or injury, danger or peril. Since nobody wants that to happen and everyone wants to limit risk, how do we measure it? After all, we learned in business school (or was it kindergarten?) that if you can't measure it, you can't manage it. Risk can be measured by a simple formula:

RISK = Capability **x** Probability

Risk is the magnitude of the bad thing, or destructive power, multiplied by the likelihood or probability of it happening. This follows in every aspect of life. The US Department of Defense makes this calculation all the time with regard to our adversaries. India and the United Kingdom have nuclear weapons, massive capability for destruction, but we believe that the risk to US national security is low. Why? Because we think that their leaders are sane and pose little likelihood that they will actually use that power in a bad way. Based purely upon capability, the United States is the biggest threat on the planet, yet very few Australians go to bed every night worrying about a US nuking. Alternately, we do worry about rogue nation states and non-nation state actors getting ahold of nuclear weapons, even at small capacity, because history has shown those factions to exhibit leadership instability and downright kookiness that jacks up the probability part of the equation for increased risk.

ISSOs manage risk by prioritizing things based upon this simple formula, trying to prevent attacks that can wipe out or co-opt the network or data, lowering the probability of attacks, or mitigating the impact of attacks by reducing the vulnerability to damage. This is a hairy problem that keeps CISOs and ISSOs up at night. Determining capability and probability are challenging, but due to limitations on the resources of time and money, this is exactly how decisions get made. In the world of federal information systems, if that overall risk becomes too high to accept, we shut applications down or don't let them even get started - no Authority to Operate (ATO).

As you can see, measuring risk involves a lot of mental calculus, weighing different variables in the context of your organization and current conditions. Risk is a broad, multi-faceted topic. Compliance is a subset of risk. If risk is like calculus, compliance is more like multiplication. Compliance has a certain, simple truth it follows, as you might see in multiplication charts. The structured, repetitive, manually demanding requirements of the act of compliance make it a perfect candidate for automation.

How compliance fits into the RISK EQUATION.

Back to Webster, compliance is defined as the act of complying to a demand or proposal. In government, compliance usually deals with a law, regulation, or a standard that serves as the bare minimum to adhere to in order to build a resilient environment and prevent chaos. Ergo, in the world of cybersecurity compliance, the federal government has determined a minimal set of practices, standards, and configuration settings for compliance that govern major elements of the overall enterprise information systems picture. The government has already determined many of the risks and vulnerabilities to respond to.

For cloud providers, compliance is rewarded with FedRAMP certification. For terrestrial applications and systems, it's the Risk Management Framework, or RMF accreditation. The criteria for these compliance standards are continually changing, because information system operations, applications, developments and threats keep changing. Keeping up with things can be daunting, and if history has taught us anything, it's that human beings tend to use new technological advancements first and then figure out how to govern them second - in this case, hopefully shortly after the fact.

Here's your "AH-HA" TAKEAWAY.

Compliance does not equal risk management. It is just an element of risk management. Remember, compliance is the minimum standard to prevent electronic anarchy. It is the baseline that serves as the you've-got-to-start-somewhere foundation that can be measured and provide some sort of consistency across your information systems portfolios. Without getting too far into the weeds here, SteelCloud is in the business of helping entities in the federal government (agencies, contractors, etc.) enforce and automate compliance for RMF accreditation. In plain speak, our ConfigOS software tool automates the scanning and remediation of those important configuration controls - and there are thousands.

These controls are governed by a baseline standard set up by a governing body of how things should work. DISA puts out their version called Security Technical Implementation Guides (STIGs) - a cybersecurity methodology for standardizing security protocols and controls within networks, servers, computers, and logical designs to enhance overall security. This standard is used by all DoD and increasingly the federal civilian world, which also uses a comparable standard published by the non-profit Center for Internet Security (CIS). The principle is the same. You've got to start somewhere. For RMF compliance, federal systems need to meet these minimum standards. This does NOT prevent all risks, but is the most meaningful, and measurable, way to start.

The beauty of these controls is that you don't have manually solve for each one. You can automate the process of scanning and remediation, leaving your cybersecurity team more available to address the larger and more complex issues of risk.

Building a compliance foundation for RISK MANAGEMENT.

Even after meeting the security baseline standard of compliance, compliance still must be managed. If you work in cyber compliance, then you know that the generic application of these standard controls tend to break application stacks. More than a few of us have spent countless hours (or days) trying to figure out which STIG control(s) is causing an issue, sending Information Assurance (IA) hit teams into the cyber cave without so much as a flashlight to illuminate their checklist of hundreds of potential culprits. When these brave detectives figure out the bad guy or guys that broke operations, they un-do the application of that control, document it in a waiver, and then submit that security package for approval with one to many acceptable risks (the waivers) that get signed off on by the person at the higher pay grade whose neck is now on the line. The point being that every application stack in the federal government will therefore have a unique secure baseline of compliance in order to operate. At SteelCloud, we call that unique baseline a security signature, implying that distinctiveness in its name.

Waivers are very important. I just called them acceptable risks, but they are a good place for ISSOs to consider risk management. Start with the most secure baseline possible for operations, and then manage risks accordingly thereafter. What can you do with that information? Now, on a very limited, reasonable number of waivers, the ISSO and their team can decide on how much risk is really there. Go back to the risk formula. This has now become a manageable workload for the limited person resources available. Too much risk, go back to the code in the DevSecOps process and deal with the problem so that control can be satisfied, and the waiver lifted.

That evaluation of risk should typically be a human-in-the-loop decision. This is where ISSOs earn their money and should be spending their time.

> *We're spending 80% of our time aggregating information and only 20% of our time actually analyzing it. That needs to be the other way around.*

Automate Compliance to Focus on RISK

What we at SteelCloud have found, and the reason we are in business and growing so fast, is that actually getting to that secure baseline takes an inordinate amount of time, personnel and money. When agencies and contractors are burning so many cycles on getting to compliance, they have little time left to truly deal with risk! And risk is the overarching issue! It is reminiscent of what one decorated Colonel in Air Force Intelligence told me in the Pentagon the day after the San Bernardino terrorist attack—"We're spending 80% of our time aggregating information and only 20% of our time actually analyzing it. That needs to be the other way around."

Exactly! Achieving that unique secure baseline should be thought of the same way, which is the foundation of SteelCloud's business. Imagine if achieving that baseline was cheap, easy and quick. What could you be doing to lock down risks if your people weren't overwhelmed by compliance? Using our automated remediate capability and detective tools, we flat out remove 70-90% of the labor and time to get you to that starting point. This is intelligent automation at its best, often termed robotic process automation (RPA). The ConfigOS software is essentially RPA for cybersecurity controls that catalyzes true risk assessment, dealing with the threats that really matter since all of the compliance concerns have been automated. However, you get there, get to cyber compliance as quickly as possible to set the foundation for your risk management practice.

Figure 1 | STIG Compliance is the Foundation for Cyber Risk Management

SteelCloud
20110 Ashbrook Place, Suite 170
Ashburn, VA 20147
1.703.674.5500
info@steelcloud.com | **steelcloud.com**

For more information on ConfigOS Command Center and to see a short product demo, visit us at **https://www.steelcloud.com/configos-cybersecurity/**