WHITE PAPER

ACHIEVING TOTAL COMPLIANCE IN THE CLOUD

Ensure Your Cloud Infrastructure is Audit-Ready for 35 Regulatory Standards with Cloud Management

CloudCheckr

ACHIEVING TOTAL COMPLIANCE IN THE CLOUD

Compliance can mean different things to different people and organizations, but the common definition is conformance to industry standards or regulations. Each industry may have its own such standards, but many organizations find themselves operating within multiple industries. For example, consider a private university that has a medical center, such as Harvard. You might not think that federal regulations apply to them, but because they deal with financial aid, they need to conform to DFARS, the Defense Acquisition Regulations System. Likewise, since they are likely to accept credit cards, even if it's just for parking, they should adopt standards from PCI DSS, the Payment Card Industry Data Security Standard. Finally, because they deal with health records, they need to obey HIPAA, the Health Insurance Portability and Accountability Act. There are dozens of such regulations, promoted by government and industry associations.

Enterprises need to focus on their core competencies, so it can be hard for them to track the status of multiple individual regulations, yet that is precisely what is required to ensure compliance. If there is a failed audit, or worse a security incident, the penalties for non-compliance can be severe, running into millions of dollars. These fees are on top of the cost of a security breach. To mediate against such threats, organizations must continuously log, audit, and protect their environments. This means dedicated resources and personnel for tasks that don't directly contribute to the bottom line.

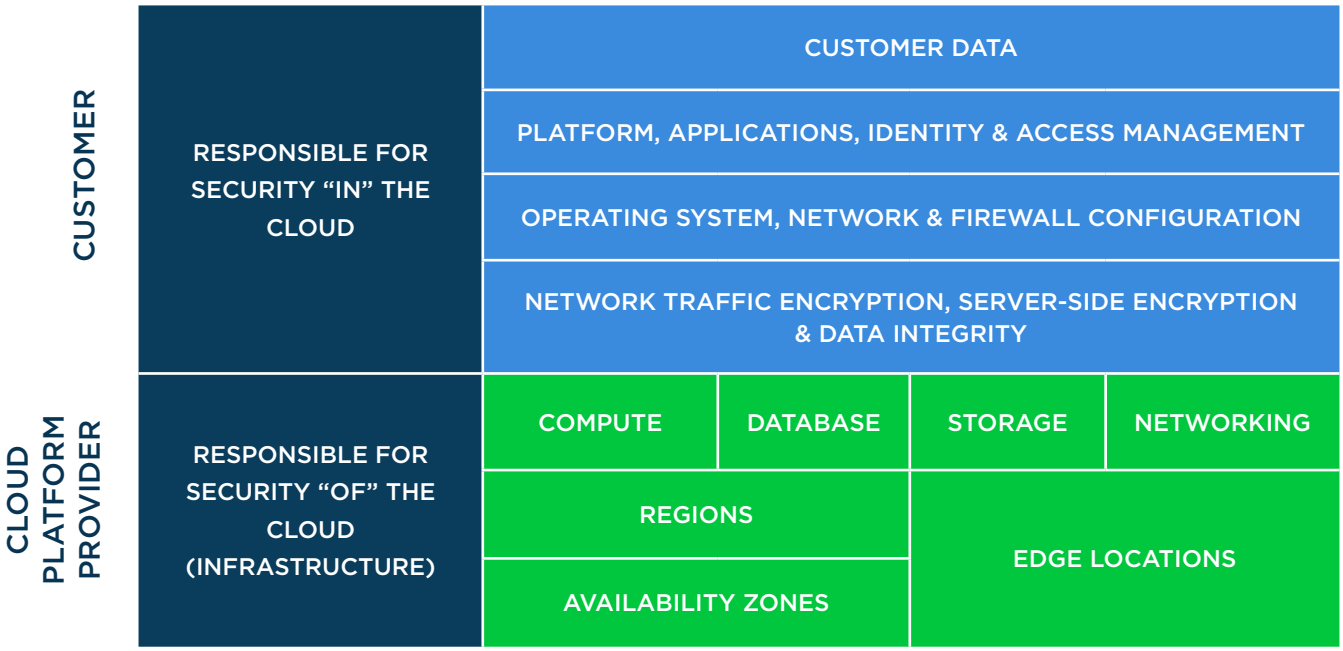
Managed Service Providers (MSPs) and Cloud Solution Providers (CSPs) as well as Value Added Resellers (VARs) can offer Compliance-as-a-Service, delivering a valuable function for which they can be rewarded. Unlike migration or other point-in-time services, compliance needs to be a continuous effort, resulting in a recurring revenue stream.

What You Can Do to Close the Gaps

Have you seen the commercial where a bank is being robbed? A bank customer begs the security officer to do something but he says "I'm just a security monitor. I only tell you if you're being robbed... You're being robbed." Monitoring is definitely an important part of a secure environment, but you also need assessment to "score" your security configuration and compliance to enforce security.

A Better Way

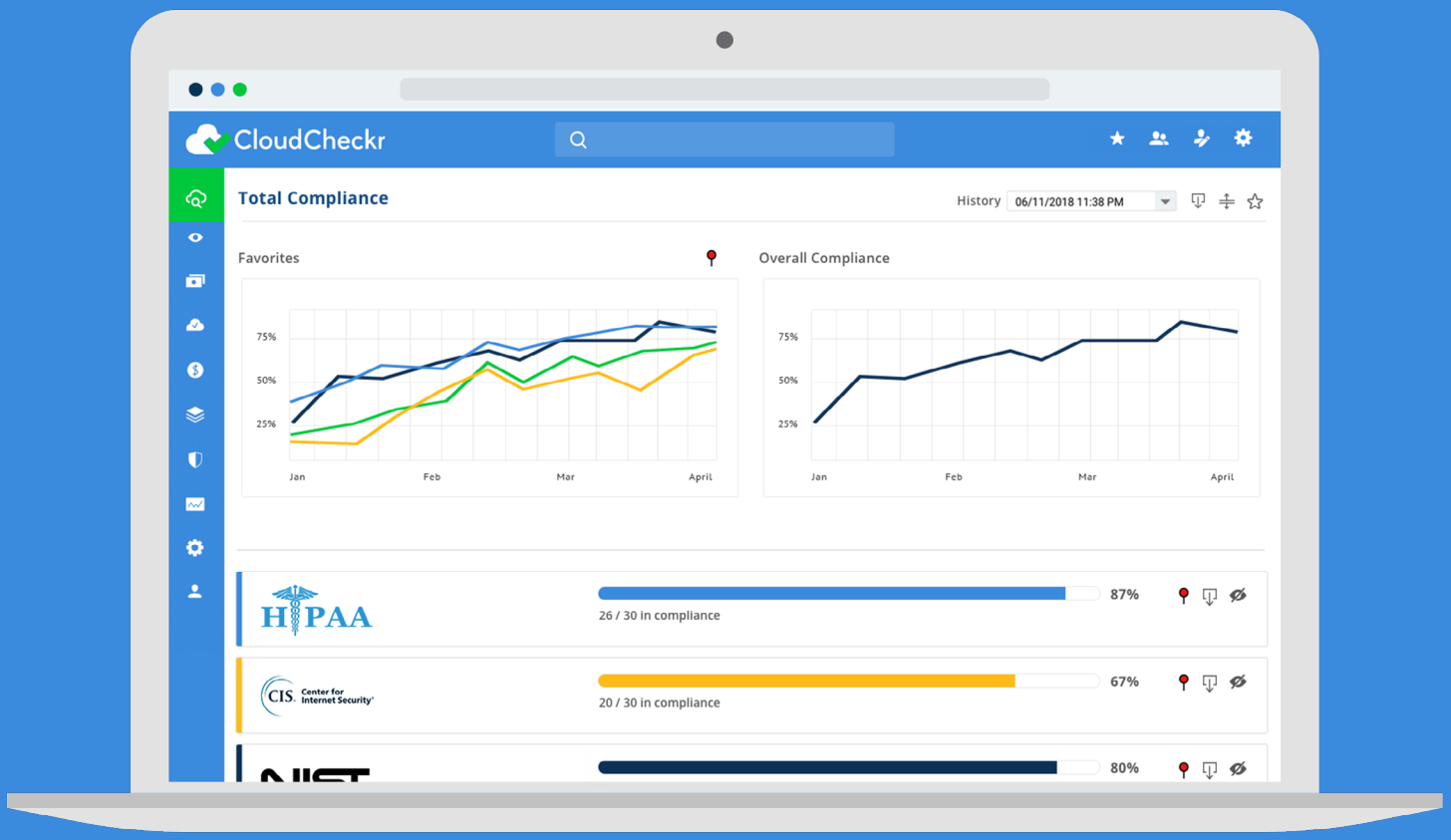
This is where technology comes in. Software and services, like CloudCheckr, can monitor and score an enterprise's security posture. This is done every day, throughout the day. Administrators can be alerted when vulnerabilities are discovered. A comprehensive compliance offering, such as CloudCheckr, includes Self-Healing Automation. This ensures that misconfigurations are corrected automatically upon detection, and the administrator is informed of the fix, even if they were asleep!



The Shared Responsibility Model, as promoted by AWS and Microsoft Azure

Shared Responsibility Model

The cloud vendors all subscribe to a concept called the Shared Responsibility Model. While they provide secure physical facilities and hardware, it is incumbent upon the cloud customer to lock-down their configurations. This is not a knock against cloud providers, who offer a wide variety of tools to ensure security and have a vested interest in ensuring the acceptance of the cloud as a secure service. Many security vulnerabilities are due to human error, wherein they take a secure, locked-down configuration and deliberately open a path to the public for some reason. A good analogy is a contractor building a solid house with strong doors and sophisticated door locks. If the homeowner leaves the door wide open, it does no good. Each of us must play our part.



CloudCheckr Total Compliance

Keeping Score

The Total Compliance report in CloudCheckr presents both a point-in-time score for over thirty regulations as well as historical graphs showing the organization's progress towards completeness. Enterprises can "favorite" the regulations that are pertinent to them, and see scores for just those favorites as well as an overall score. The goal, naturally, is to get to 100% and to stay there. That's where CloudCheckr's 550+ Best Practice Checks come in.

AICPA GAPP

AICPA SOC2, SOC3, TSPC

ANSSI - 40 Measures

Australian Essential 8

Australian Top 35

CIS

COBIT 5

CoM 201 CMR 17.00

CSA CCM v3

DHS CDM Program

FFIEC Booklet 2016

FFIEC CAT

FY15 FISMA Metrics

HIPAA

IEC 62443-3-3-2013

IRS Pub1075

ISO 28002-2013

ITIL2011 KPIs

NERC CIP v5

NERC CIP v5

NERC CIP v7

NIST 800-171

NIST 800-53 rev4

NIST 800-82 rev2

NIST Cybersecurity Framework

NIST SMB Guide

NSA MNT

NSA Top 10

NV Gaming MICS

NYCRR 500

PCI DSS 3.2

Saudi AMA

SEC OCIE Audit Guide for AWS

SG MAS TRM

Victorian PDSF v1.0

CloudCheckr tracks and scores more than 30 compliance frameworks

Check Your Cloud

CloudCheckr provides access to hundreds of Best Practice Checks categorized by Cost Savings, Security, Availability and Utilization. Each check is classified as High, Medium or Low importance, and color-coded red, orange, and yellow accordingly. Many of these checks can be customized. For example, one such check is the Stale Password Check. An organization can decide if that means passwords should change every 180 days, or 90 days or something altogether different.

Checks can trigger notifications via Slack, SNS, PagerDuty, ServiceNow, Jira and email. Custom Best Practice Checks can also be configured to launch a Lambda function. The real power comes from the self-healing capabilities available for many of these checks. An administrator can select Fix Now to have the identified issue corrected immediately. Another option is Always Fix, which tells CloudCheckr to fix the same issue every time it comes up, automatically. Some users may not have the experience to be trusted with Fix Now, in which case they can leverage CloudCheckr's Workflow Automation functionality. In this scenario, such users will see a Request Fix button which sends the request to their manager or co-workers who can determine if the fix is warranted.

It is worth noting that regulations often include non-software controls, such as how paper records are dealt with and how employees are trained. CloudCheckr naturally focuses on software-defined controls. A score is generated based on the percent of such controls that are in compliance.

Conclusion

There are a number of strategic and competitive advantages to addressing a compliance program as an opportunity rather than a burden. Part of the answer is knowledge and attitude. Approaching the compliance program with a good understanding of these benefits will improve company security and possibly sales operations, marketing traction, and the bottom line.

ABOUT CLOUDCHECKR

CloudCheckr's sophisticated cloud management platform offers Cost Optimization, Billing & Invoicing and Security & Compliance in a single pane of glass across infrastructure to ensure total security and compliance, while optimizing cost and expenses. With continuous monitoring, 550+ best practice checks, and built-in automation, CloudCheckr enables IT, Security, and Finance teams to manage their cloud environments with confidence. Government organizations and Global 2000 enterprises trust CloudCheckr to deliver the most robust cloud management platform in today's marketplace.

Need CloudCheckr for your organization? Learn more at **www.cloudcheckr.com**.

CloudCheckr

342 N GOODMAN ST,
ROCHESTER, NY 14607

1-833-CLDCHCK

www.cloudcheckr.com

Updated August 10, 2018