CISO MAG

beyond cybersecurity

Volume 4 | Issue 11 | November 2020

COMPLIANCE & RISK MITIGATION STRATEGIES

FRIEND OR FOE?

Today's cyber-attackers are masters of disguise.

Sophisticated email attacks, compromised cloud systems, vulnerable devices - it's hard to predict tomorrow's threats. AI can distinguish between legitimate activity and an emerging cyber-threat, and fight back in seconds.

DARKTRACE
World-Leading Cyber AI

CISO MAG
beyond cybersecurity

Volume 4 | Issue 11
November 2020

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Principal Editor
Brian Pereira
brian.p@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Feature Writer
Pooja Tikekar
pooja.v@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Deputy Business Head
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Publishing Sales Manager
Vaishali Jain
vaishali.j@eccouncil.org

Design and Marketing
Rajashakher Intha
rajashakher.i@eccouncil.org

Executive – Marketing and Operations
Munazza Khan
munazza.k@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Image credits: Shutterstock
Cover & Layouts by: Rajashakher Intha

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Brian Pereira.
The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & SEPTEMBER not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof SEPTEMBER be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.

EDITOR'S NOTE

COMPLIANCE IS NOT A CHECKBOX EXERCISE

According to a recent survey of North American CISOs, CISOs are preparing for an average of 3.3 security compliance standard audits over the next six to 12 months. These mandatory assessments require significant financial and operational investments. A typical cybersecurity assessment can cost tens of thousands of dollars and months spent with third-party auditors. It is no small undertaking for any organization, regardless of its maturity or budget.

With that in mind, security leaders should seek to get the maximum value from these assessments, writes **AJ Yawn**, Cloud Security Expert and NABCRMP Board Member in *"CISOs Must Declare an End to the War between Security and Compliance,"* which you will find on page 20 in this issue. But the unfortunate reality is that cybersecurity audits are viewed as "check-the-box" exercises where auditors are paid to produce a report, so the Board, executives, and interested third parties (customers and vendors) feel good about the perceived security status of the organization. It isn't acceptable when these assessments are expensive, time-consuming, and extremely important to the bottom line.

Meeting a particular compliance framework or standard does not mean you are secure or won't be breached. There's a Smörgåsbord of standards that leaves the CISO confused and bewildered, writes **Chaitanya Kunthe**, Co-founder and Chief Operating Officer at Risk Quotient in *"How Organizations Should Adopt Changing Compliance Standards,"* on page 46 of this issue. Read his article to find out more about compliance standards and frameworks, and how these are evolving.

Narendra Sahoo, Founder and Director of VISTA InfoSec says it is not easy to ensure data sanctity and security with a third-party. Cloud service providers find it challenging to comply with various data security and privacy regulations. He believes SOC 2 compliance will help cloud service providers to secure data in the cloud. Read all about its benefits in his article *"SOC 2 Compliance and Cloud: What You Should Know,"* on page 62.

Speaking of third parties, **Alla Valente**, Analyst at Forrester, says the complexities and consequences from third-party relationships are increasing. What adds to the complexity of the third-party ecosystem is that although companies have limited or no control over how third parties secure their technology infrastructure, applications, or data — they're fully responsible for security, privacy, or regulatory missteps that occur during the relationship. Be sure to read her risk mitigation strategies in *"Innovate Through Uncertainty by Managing Third-Party Risk,"* on page 38.

Finally, the centerpiece of this issue: A story about how Google is trying to simplify compliance for governments and the public sector in the cloud. Read the cover story written by **Jeanette Manfra**, Director for Government Security and Compliance, Google Cloud Office of the CISO, on page 70.

We hope you enjoy reading the other articles in this issue as well.

Please write to us at editorial@cisomag.com or cisomag@eccouncil.org.

Jay Bavisi
Editor-in-Chief

Market Trends Report

Endpoint Security Survey

Take Our 5 minutes Survey
& Get CISO MAG Annual Subscription

TAKE SURVEY NOW!

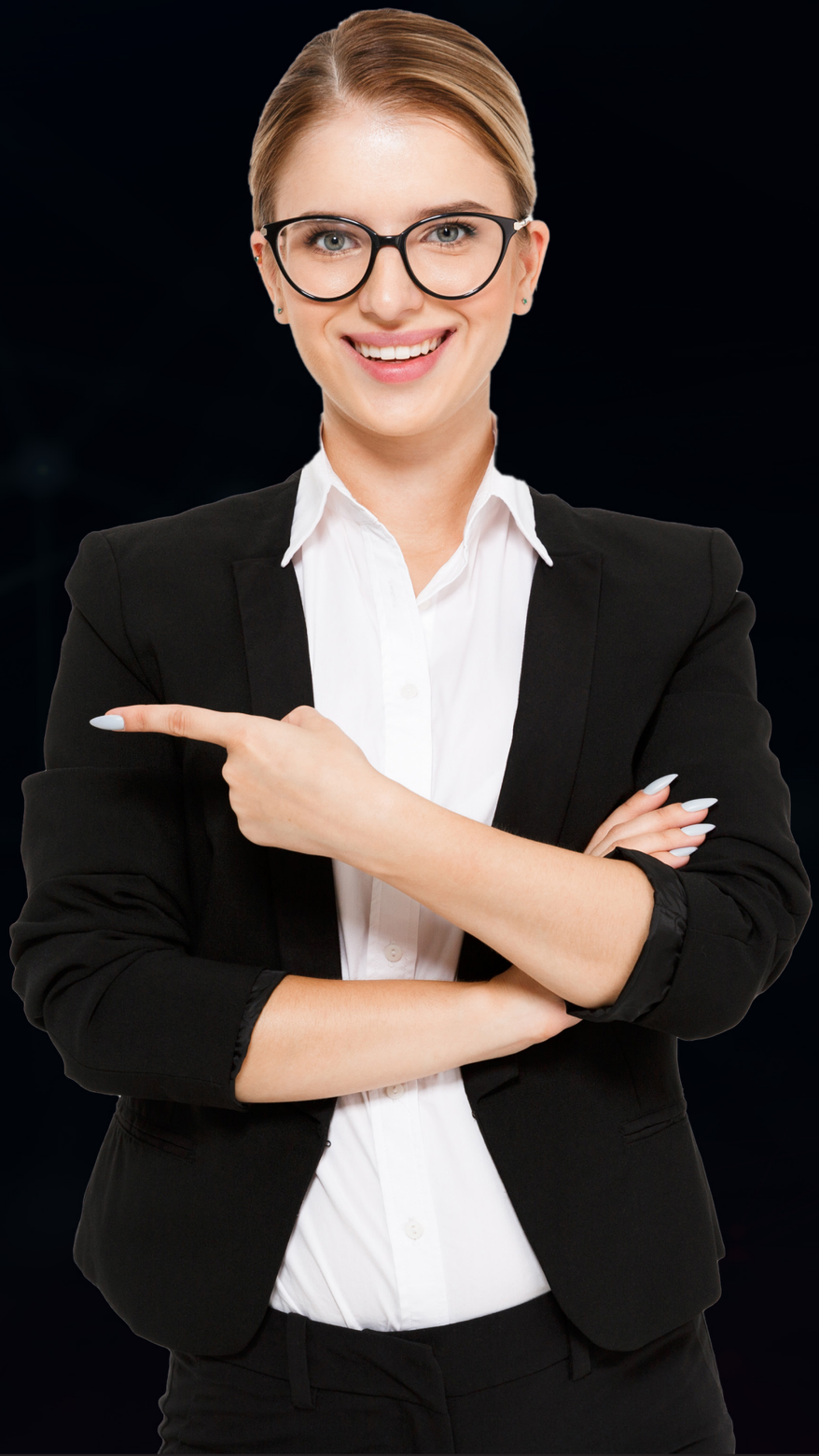
Get **CISO MAG Annual Subscription Worth $149** for **Free**

Get 30 Days **CodeRed** Subscription*

Exciting Weekly Prizes

2 lucky winners will get **Amazon coupon of $15**

2 Lucky winners will get a **chance to write for CISO MAG**



INDEX

EMPHASIZE THE **"SPIRIT"** OF COMPLIANCE OVER SIMPLY **"CHECKING ALL THE BOXES"**

Bryan Cline
Ph.D., Chief Research Officer,
HITRUST

Vol 4 - Issue 11

If you're about to face a compliance audit, undergo an assessment, or produce an industry certification — and are doing so without much serious consideration for what it means to embody information security and data privacy throughout the organization — you are likely missing the forest for the trees. If the actions taken are solely about achieving certification and remain unclear and impractical from the intent of the regulatory requirements, what you don't see can come back to haunt you.

Compliance isn't supposed to be about ticking a bunch of checkboxes, which when "completed" represents a binary result: pass or fail. What may not be as clear, even by achieving compliance, is that you may still be left with substantial exposure to compliance risk.

In effect, by simply achieving the letter of compliance, you leave your company unnecessarily exposed to business risk: plain and simple. There is residual risk in the continuum that falls between doing the bare minimum to address compliance requirements and doing what is actually needed to address the intent of the requirements: providing a reasonable level of due diligence and due care.

The Three Levels of Compliance Maturity

Achieving a risk score isn't the solution. Neither is ticking a bunch of non-verifiable checkboxes. The correct solution involves moving beyond the binary state of the letter of compliance and, instead, striving to achieve compliance in a way that meets the intent of the regulations and standards. To get to the right solution, let's first take a broad view at three levels of compliance maturity.

1. **Zero visibility and disorganized control**

   At this level, businesses are subject to maximum unmitigated exposure. IT risk assessments are limited as most regulations are concerned with information security (more so than IT) and individual privacy, which information security supports. The business is likely stuck at this maturity level because there is an unclear association between compliance risk, information security risk, privacy risk, and business risk.

2. **The letter of compliance is achieved**

   Organizations that reach this level recognize the connection between information risk and business risk but have minimum mitigations in place. At this level, compliance risk still exists as organizations have implemented an incomplete set of controls, and many times, those that have been implemented fail to meet the outcomes intended by the regulation — as interpreted by the regulator.

   The drivers to achieve this level include the risk of fines, penalties, and loss of business. Many businesses choose to stop at this level because compliance is enough, and the self-assessments show everything is OK; after all, the letter of compliance was achieved.

3. **Intent to protect is embodied throughout the organization**

   Those that reach this level have an understanding of risk and visibility into how it can affect the business. Furthermore, that risk is sufficiently mapped to business risk and paired with proactive controls and responses designed to meet the letter of compliance and support, with a clear and focused goal of keeping the company's information safe, which is often the intent of information security and individual privacy regulations. The common drivers that cause organizations to reach this level often include direct experience with a breach, awareness of a breach at another company, or the loss of business due to an inability to articulate proactive risk management. Perhaps it's time organizations don't wait for one of these negative drivers to surface before taking action.

Achieving an Appropriate Level of Assurance

But even if you are following the spirit of compliance, you may not be able to adequately demonstrate compliance when a regulator comes knocking at your door. For example, self-assessments are generally less trustworthy than independent assessments and are almost always inflated due to a lack of understanding of the requirements and a desire to cross the finish line to pass an audit or close on new business.

Ultimately, though, compliance boils down to achieving an appropriate level of assurance:

- What level of assurance do you want to achieve?
- What level of assurance can you demonstrate?
- Can you demonstrate assurance to ALL stakeholders?

Then consider whether you have provided the level of assurance you want and that your stakeholders require. Have you gone beyond ticking the boxes of compliance, or is it just a charade?

The Three Dimensions of Intent-Driven Assurance

To answer these questions, we will explore the three dimensions of assurance and the attributes associated with each:

1. **Suitability:** The controls must manage risk to a level deemed acceptable by the organization, not just what is described in the regulation(s) you are managing to.

2. **Impartiality:** For both the letter of compliance and the intent of compliance, independent assessments are more trustworthy than a self-assessment, and help improve the level of assurance provided.

3. **Rigor:** The results must accurately reflect the organization's information security posture as it relates to the regulatory requirements.

Each of these dimensions of assurance is supported by multiple quality attributes of an approach that contributes to the reliability of the assurance. This is what we at HITRUST® and our numerous councils and committees refer to as "rely-ability." The answers to the questions below — as they pertain to each of these attributes — will address whether various aspects of the assurance approach are sufficient to move into a world of intent:

- Transparent – Can you share where and how you arrived at your current assurance level?
- Comprehensive – Do your controls address all reasonably anticipated threats?
- Prescriptive – Are the controls detailed enough to ensure their implementation achieves desired information protection objectives?
- Accurate – Do the results accurately reflect your security posture and provide a higher level of assurance?
- Scalable – Can your assurance approach be used by organizations of different types and sizes in different industries?
- Efficient – Can your assurance approach be leveraged by multiple relying parties?

It's also a good idea to check for consistency. Was your assessment performed in accordance with the standard and independently repeatable assessment and reporting requirements?

Use-Case Examples of Ignoring the Spirit of Compliance

Let's look at two use-cases that illustrate how risk is often left behind and where the spirit of compliance is completely ignored. And perhaps, even the letter (and achievement) of compliance is still missed:

Use-Case #1 - Risk Analysis

Take, for example, the risk analysis requirement from the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (HSR). Did you do a risk analysis as required? Does it address all reasonably anticipated threats? Does it address all electronic Protected Health Information (ePHI) in your environment? Do the controls you implement address the intent of the risk analysis, which is to specify controls that will provide for the adequate protection of ePHI?

If you only address major Electronic Health Record (EHR) systems and not the "rogue IT" under your medical researchers' desk, or if you can't demonstrate your threat analysis and control specification process because the CISO that did that for you left five years ago, you may very well have a problem.

The letter of compliance may have been met, but when checking to determine how well your implementation achieves the regulatory intent, the truth comes out. And in this case, you may have thought you met the letter of the requirement but, in fact, you not only missed the intent of the requirement but also the letter.

Use-Case # 2 - Workforce Awareness Training

Do you have a workforce training program? If so, how often is the program executed? Are there exceptions for how often and for whom the training is conducted? Are there corrective actions taken? Answers to each of these questions