THE STATE OF NONCOMPLIANCE IN CYBER RISK MANAGEMENT

COMPLIANCE AND ITS RELATIONSHIP TO RISK POSTURE

riskrecon
mastercard

Cyentia INSTITUTE

Key Findings

ISO/IEC 27001 is proven to be the most difficult standard for organizations to pass.

A host in the cloud is 19% less likely to have compliance issues than on-premises hosts

Web app security is the most common criteria issue found among the regulations studied

Education has the highest number of noncompliant findings across all industries

INTRODUCTION

Many cybersecurity veterans will be quick to share the common wisdom that compliance does not equal effective cybersecurity risk management. But is there any truth behind this wisdom, or is it more of a symptom of the too often adversarial relationship between auditors and system administrators? Do compliance requirements lead to measurable benefits to risk management?

Cybersecurity regulations and frameworks, authored by a bevy of government and industry oversight groups, provide a barometer for baseline security best practices. Whether they're coming from the PCI Council, NIST, ISO, or CIS, the requirements laid out by these compliance groups offer a reference point from which organizations can use to chart their security risk posture journey.

CHECKBOX COMPLIANCE:

THE FOLLOWING OF THE BARE MINIMUM OF COMPLIANCE STANDARDS

Checkbox compliance — the following of the bare minimum of compliance standards — surely isn't a path leading to a robust risk management posture. At the same time, if we accept compliance risk (the threat of failing a mandated compliance regime and suffering adverse effects) as an element of an organization's overall cyber risk, then it's not unreasonable to suspect that a failure to manage this aspect of risk may well correlate with challenges in other parts of the risk profile.

COMPLIANCE RISK:

THE THREAT OF FAILING A MANDATED COMPLIANCE REGIME AND SUFFERING ADVERSE EFFECTS

While auditors may be the arbiters of how much headway an organization is making on its compliance-driven security improvements, relying solely on the auditor's evaluations is a high-stakes, zero-sum game. Breaking down requirements into meaningful components and taking a progress-not-perfection approach can help facilitate meaningful continuous improvement both for cyber compliance and risk management. Stepping away from the proverbial mirror and getting a feel for how well an organization's peers are complying with regulatory and framework standards can also provide some valuable insight

The big obstacle is that it can often be difficult to gauge how well an organization is performing compared to its peers. While some organizations may list the standards they follow, getting access to their performance through auditors' reports is not generally possible. To that end, RiskRecon offers risk and compliance decision makers a peek under the covers to see how well the "other guys" are doing.

THE GOAL OF THIS REPORT IS TO OFFER A VIEW ON THE STATE OF COMPLIANCE IN TODAY'S TYPICAL ORGANIZATION, INCLUDING:

The rate of noncompliance among a typical organization's assets

The compliance standards that are hardest for organizations to adhere to

How well compliance tracks against the overall risk surface

The most common security controls causing non-compliance

Where does the data come from?

RiskRecon is able to offer this analysis based on findings from its cybersecurity ratings and assessment platform. This compliance report examines the security assessment results for tens of thousands of organizations around the world, and then mapping them to nine different modern cybersecurity compliance standards:

CIS CONTROLS V7
CIS Critical Security Controls

NIST 800-171 REV 2
Protecting controlled unclassified information in nonfederal systems and organizations

SIG LITE 2020
Abbreviated Lite requirements (2020 edition)

ISO 27001:2013
Information security management systems requirements

PCI DSS 3.2.1
Payment Card Industry Data Security Standard

SIG LITE 2021
Abbreviated Lite requirements (2021 edition)

NIST CSF V1.1
NIST Cyber Security Framework

SIG CORE 2021
Shared Assessments Standardized Information Gathering (core)

GDPR PRIVACY
General Data Protection Regulation

The mapping is fairly intuitive, since the checks done by RiskRecon's third-party assessments cover many practices similar to those stipulated by the regulators. These include security requirements such as enabling email authentication, patching software and servers, and utilizing effective web encryption.

The caveat is that the data presented here is not as tightly scoped as an auditor's assessment. While this is not a full audit of the tens of thousands of organizations in our dataset, we believe this to be a reasonable proxy to understand the types of issues organizations are struggling with. To help single out the things that matter the most, we focus on high value assets—which are also more likely to be in scope for audit findings. We recommend reading this report with the understanding that while this data isn't an ironclad reading of compliance, it does offer reasonable indications of the nature of challenges that organizations today face in meeting compliance demands.

FOCUS AREA:

HIGH VALUE ASSETS WHICH ARE ALSO MORE LIKELY TO BE IN SCOPE FOR AUDIT FINDINGS

DIGGING INTO THE REALITIES OF NONCOMPLIANCE

One of the main themes that immediately surfaces from the available data is that nearly every organization struggles with at least some degree of noncompliance.

The global data in Figure 1 below shows that between 99.4% to 100% (yes, virtually every one[1]) of the tested organizations have at least one finding that puts their assets at risk of noncompliance across eight of the nine tested regulatory frameworks.

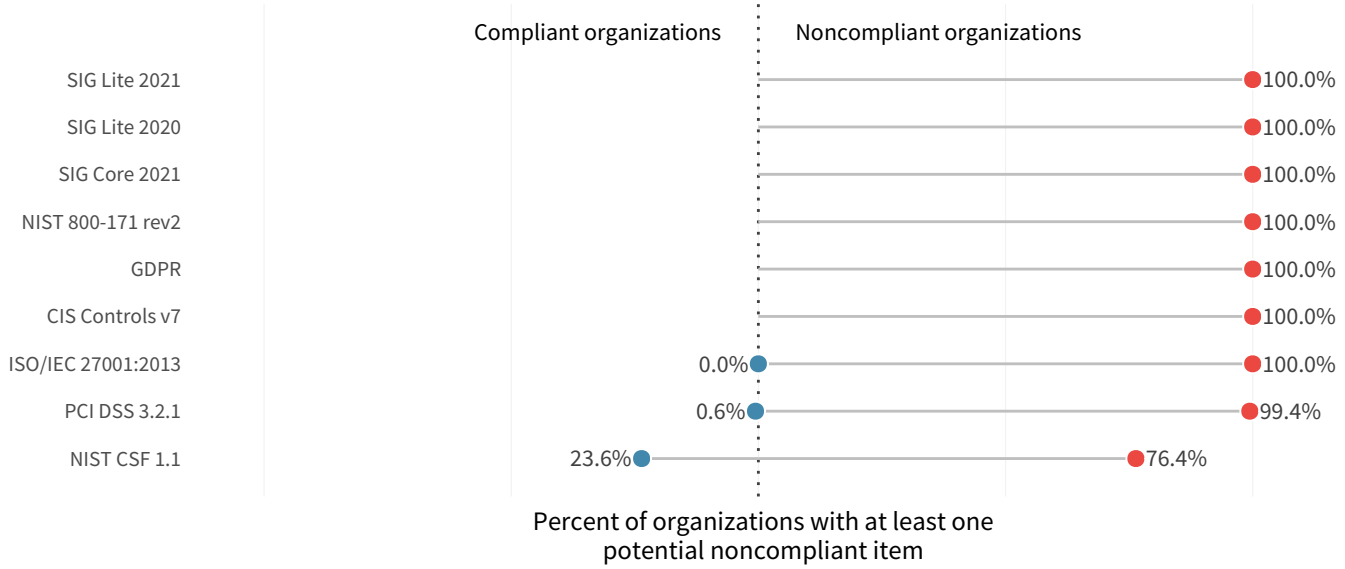


FIGURE 1: ALMOST ALL ORGANIZATIONS HAVE SOME NONCOMPLIANT ITEMS FOR EVERY STANDARD

Now, this kind of absolutist view is not nuanced—clearly this does not mean that all organizations are entirely noncompliant with all of these major standards! The problem is that this basic calculation is binary. Having even one issue on one asset will put that organization in the noncompliant bucket. This isn't necessarily how auditors or risk managers operate—security isn't a game of perfection, after all—so it doesn't offer a full picture of how far out of compliance an organization is. After all, an asset with only one compliance violation may not raise an auditor's eyebrow, but the situation may change as the number of noncompliant items rises.

FOCUS AREA:

BETWEEN 99.4% TO 100% OF THE TESTED ORGANIZATIONS HAVE AT LEAST ONE FINDING THAT PUTS THEIR ASSETS AT RISK OF NON-COMPLIANCE ACROSS EIGHT OF THE NINE TESTED REGULATORY FRAMEWORKS.

ALMOST ALL ORGANIZATIONS HAVE NONCOMPLIANT ITEMS FOR EVERY STANDARD

To be more useful, we reframe things a bit and assess the distribution of organizations based on the percentage of failed test items they experienced. Each item is a particular check for an issue, with some standards having multiple checks for each individual requirement. These are broken down by each compliance standard in Figure 2.

FOCUS AREA:

THE MAJORITY OF TESTED ITEMS SHOW POTENTIAL NONCOMPLIANCE IN ORGANIZATIONS AND A WIDE VARIATION FOR MANY STANDARDS.

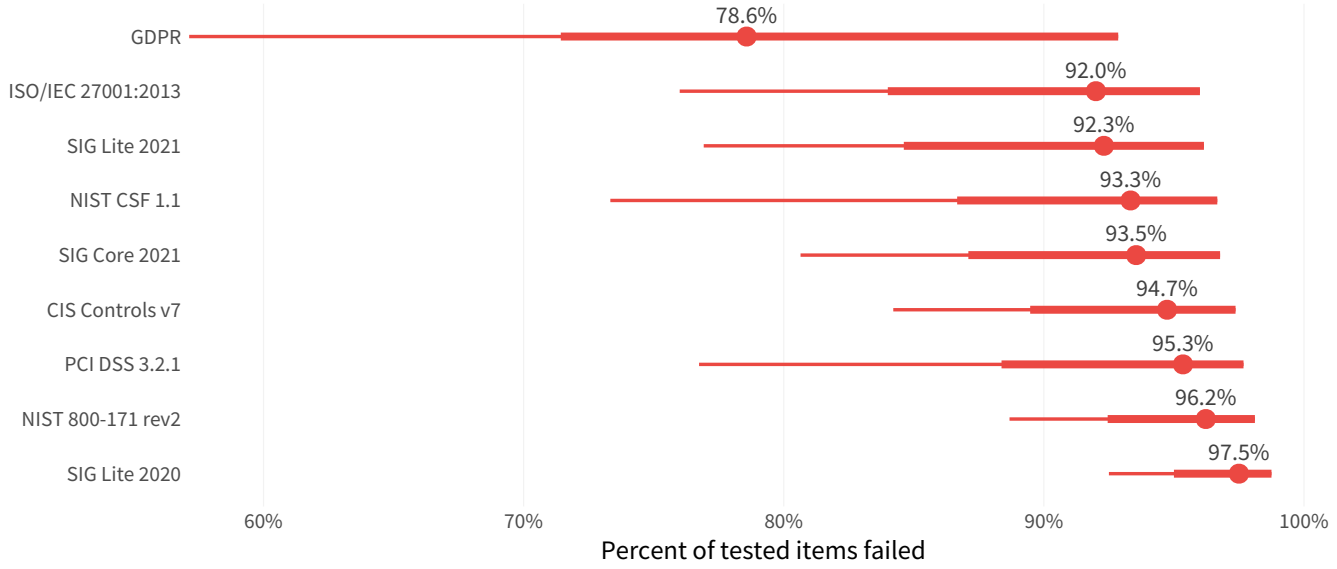


FIGURE 2: DISTRIBUTION OF PERCENT OF FAILING TEST ITEMS PER STANDARD

FOCUS AREA:

MOST ORGANIZATIONS STRUGGLE WITH THE TESTABLE ITEMS FROM THE SIG LITE 2020, NIST 800, AND PCI REQUIREMENTS.

THEY ARE MORE SUCCESSFUL WITH ISO 27001 AND GDPR STANDARDS—BUT THERE IS HUGE VARIABILITY, PARTICULARLY WITH GDPR.

With this formulation, we start to get a bit more resolution in the data. The dots on the charts indicate the median points, showing that the majority of tested items show potential noncompliance in organizations. The bars on the chart indicate the range of items tested as noncompliant, showing a wide variation for many standards. Based on the compliance breakdowns, most organizations struggle with many more of the testable items from the SIG Lite 2020, NIST 800, and PCI requirements, while they are more successful with ISO 27001 and GDPR standards—but there is huge variability, particularly with GDPR.

Compliance in the Cloud

One worthy side note here is the relationship in compliance for cloud-hosted assets versus those systems hosted on premises. The data below shows that a host in the cloud is significantly less likely to have compliance issues than on-premises hosts.

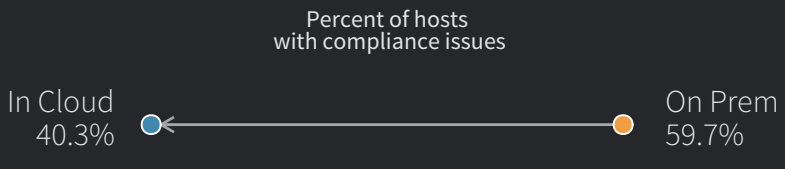


FIGURE 3: CLOUD VS ON-PREMISE COMPLIANCE

THIS PROVIDES YET ANOTHER DATA POINT THAT SUPPORTS THE RISK AND COMPLIANCE BENEFITS OF MOVING TO THE CLOUD.

Which Standards Are the Most Difficult for Organizations to Pass?

While many standards overlap to a varying degree, every standard has a different number of security requirements associated with it. Our next analysis aims to uncover how the volume of requirements for each standard impacts the rate of noncompliance across our sample. This can help us gauge which standards are more difficult to achieve.

In Figure 4, we take a look at the percentage of the requirements for each standard that are marked as noncompliant across different organizations. We see that GDPR is extremely uniform, ISO is largely problematic, while NIST CSF has the lowest amount of relative noncompliance.

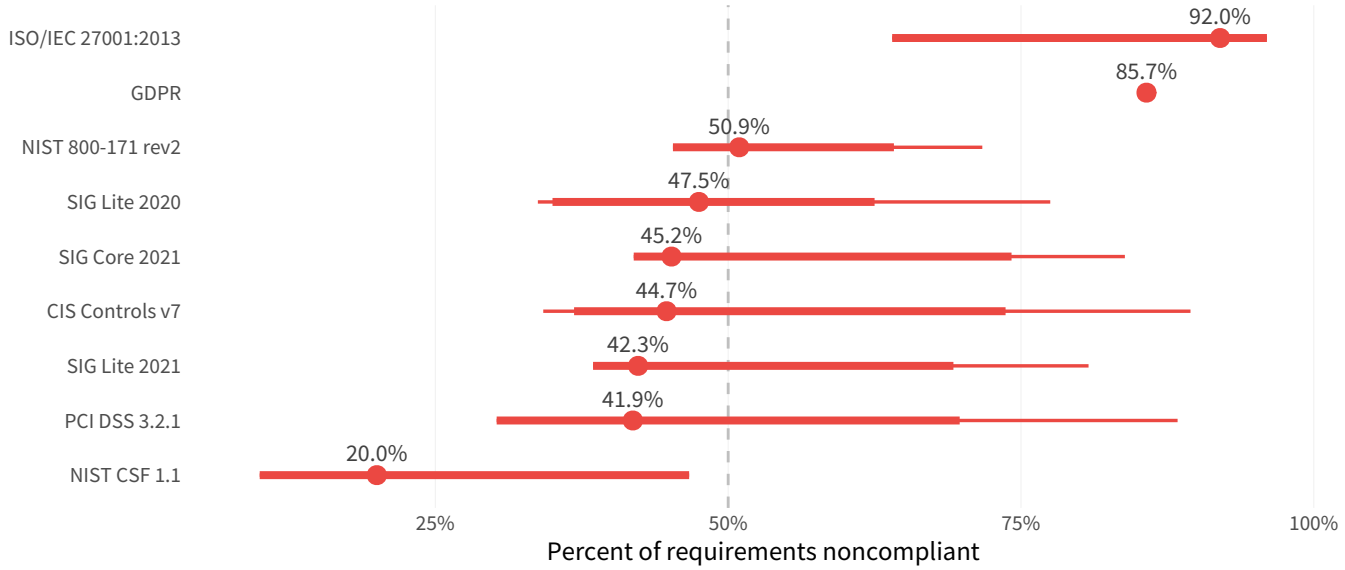


FIGURE 4: DISTRIBUTION OF NONCOMPLIANT REQUIREMENTS PER STANDARD

The median indicates the typical proportion of controls that aren't being met. The full range of lines shows where most (50%) organizations fall. Looking at SIG Core 2021, we see that the typical organization has potential issues with just over 45% of these requirements, while 50% of organizations are somewhere between 42% to 71% potentially noncompliant. As is often the case, a single number is not a good measure for all firms.

FOCUS AREA:

THE TYPICAL ORGANIZATION, USING THE SIG CORE 2021 STANDARD, HAS POTENTIAL ISSUES WITH OVER 45% OF REQUIREMENTS

FOCUS AREA:

NIST CSF INDICATES THE HIGHEST LEVEL OF COMPLIANCE

Interestingly, the NIST Cybersecurity Framework (CSF) indicates the highest level of compliance among the standards shown here. We suspect that's partly because its requirements are fairly broad, since it was designed more as a set of control guidelines, than a prescriptive checklist.

Payment Card Industry Compliance (PCI), Standardized Information Gathering Lite (SIG Lite), Center for Internet Security (CIS), and SIG Core, all are hovering close together, bringing in the middle ground of compliance. This may indicate that the requirements are a little more prescriptive and rigid, however, there are guidelines that are relatively attainable. ISO 20071 has the highest percentage of requirements that are potentially noncompliant, which is not surprising given that this standard requires buy-in and compliance in almost every single part of a company.

WHAT'S IN SCOPE, THOUGH?

With this sort of outside-in visibility, we have to account for the fact that at least some of the findings will be on low-value assets, which aren't in scope for audit. They may not even necessarily put the organization at risk of lateral movement if other mitigations such as segmentation are in place. To take the analysis to another level we now narrow the lens to focus on high-value assets.

FOCUS AREA:

WHEN FOCUSED ON ONLY THE HIGH-VALUE ASSETS, ALMOST EVERY COMPLIANCE STANDARD HAS A RATE OF NONCOMPLIANT ORGANIZATIONS OF ABOUT 12%

While we don't know which regulatory standards govern each organization, nor which of the assets or hosts are in scope for specific compliance mandates, we can make some reasonable assumptions about business criticality based on what the assets do. RiskRecon can discover what types of data collected by assets. When this information includes sensitive data like user credentials, email addresses, and credit card numbers, the assessment engine categorizes a system as a high value asset. With many of our standards taking a data-centric approach (cardholder data in the case of PCI, PII in the case of GDPR, etc.), these indicators of high-value are reasonable proxies to identify the assets that are more likely than others to be in scope.

With that in mind, we turn to look at the percentage of organizations with noncompliant findings on a high-value asset. The numbers go down, once we consider the criticality of systems. In Figure 5, we focus only on the high value assets. With this lens, almost every compliance standard has a rate of noncompliant organizations of about 12%. The one exception is NIST CSF, for which that rate goes down to just over 8%.

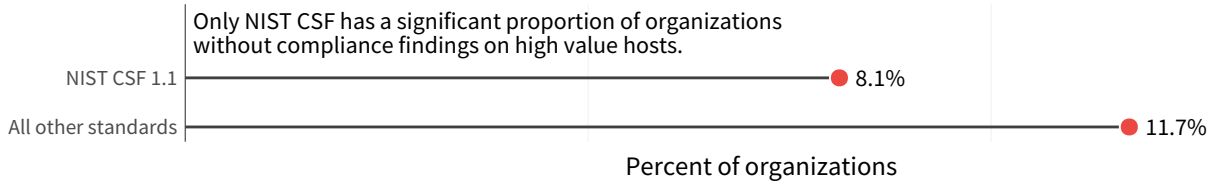


FIGURE 5: ORGANIZATIONS WITH NONCOMPLIANT FINDINGS ON HIGH-VALUE ASSETS

Lest we get too optimistic about these numbers, let's look at the rate of noncompliance on the assets and hosts themselves. This data is a little more sobering, as the majority of high-value assets — over 80% — have at least one noncompliant finding on them. NIST CSF is the exception here as well, with under 20% of high-value assets showing some evidence of noncompliance there.

FOCUS AREA:

NOT EVERY ORGANIZATION RUNS HIGH-VALUE ASSETS, BUT AMONG THOSE THAT DO, THE RATE OF NON-COMPLIANCE IS STILL VERY HIGH.

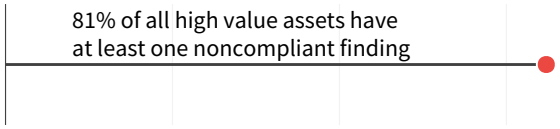


FIGURE 6: PERCENT OF HIGH VALUE ASSETS WITH AT LEAST ONE NONCOMPLIANT FINDING

The difference between this chart and Figure 5 indicates that not every organization runs high-value assets, but among those that do, the rate of noncompliance is still very high. The good news is that the binary indications of noncompliance are not as universal on these assets as on the entire sample, which means at least some level of attention is being paid to the in-scope assets.

Another variable to consider is that organizations differ in size, with some operating with just a few hosts under their care, and others running several orders of magnitude more assets. This means, an organization could potentially have a large number of findings, but it may not be a big deal if those assets are spread out across a lot of hosts. But another organization with a similar number of findings clustered within fewer hosts could be operating under a much more acute state of noncompliance (and risk!). To normalize the data a bit, we looked at the data based on the density of noncompliance, in other words, the number of compliance findings on high value hosts divided by the total number of high value hosts at organization. This provides a better understanding of the scope of the issues. This gives us the view in Figure 7.

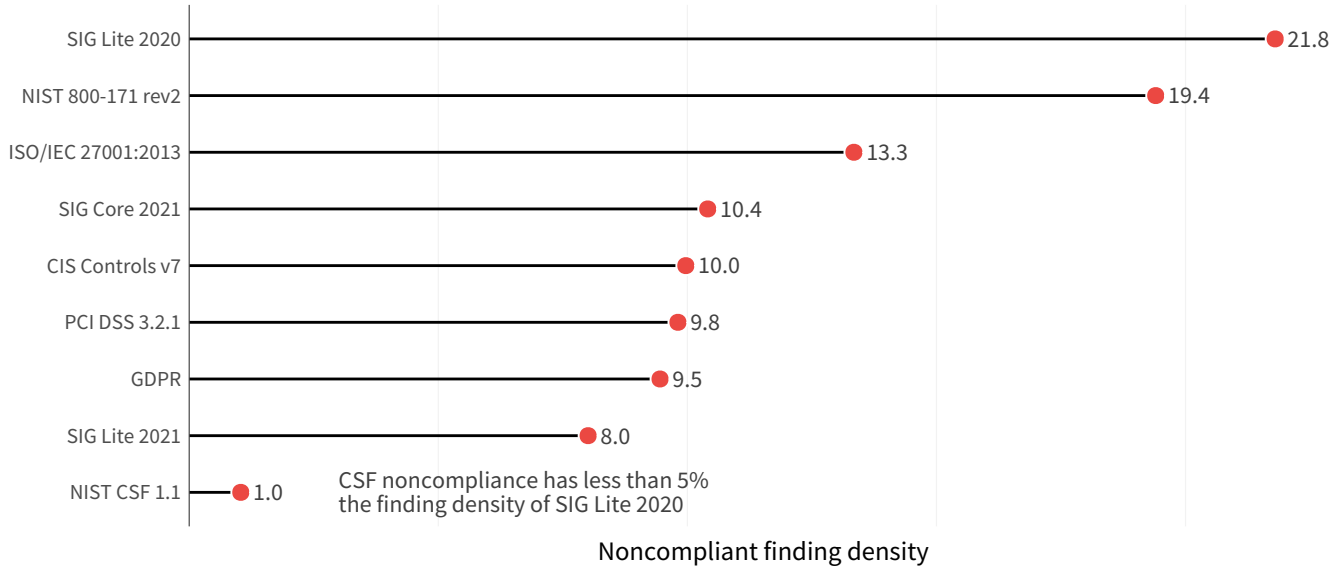


FIGURE 7: NON-COMPLIANT FINDING DENSITY IN ORGANIZATIONS WITH COMPLIANCE FINDINGS

In Figure 8, we can focus on the PCI-DSS top level requirements to better see the differences. Organizations with issues in the testing of systems and processes have 38 times the finding density compared to that of organizations that have issues with protection against malware.

FOCUS AREA:

ORGANIZATIONS WITH ISSUES IN THE TESTING OF SYSTEMS AND PROCESSES HAVE 38 TIMES THE FINDING DENSITY

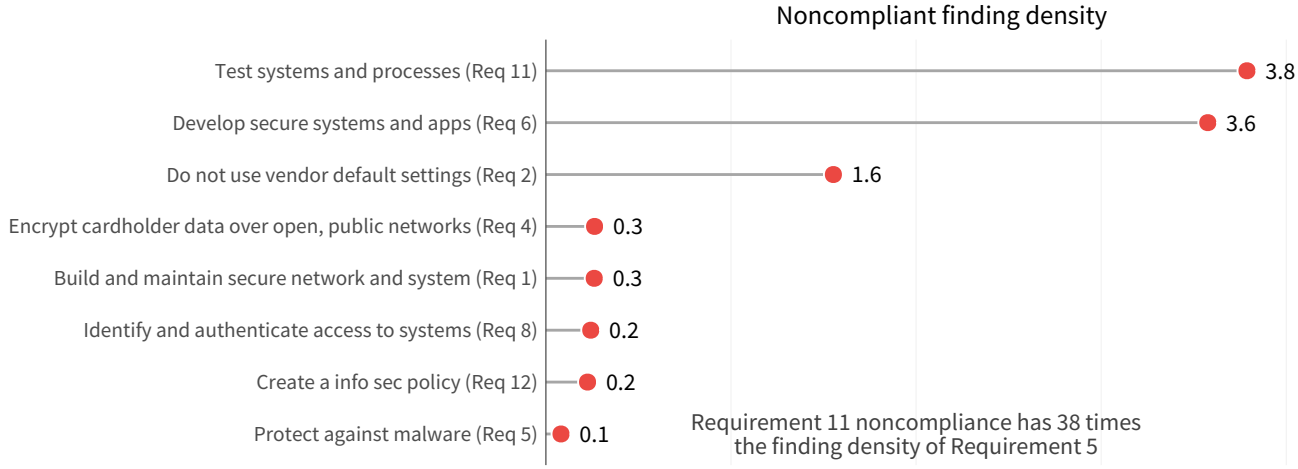
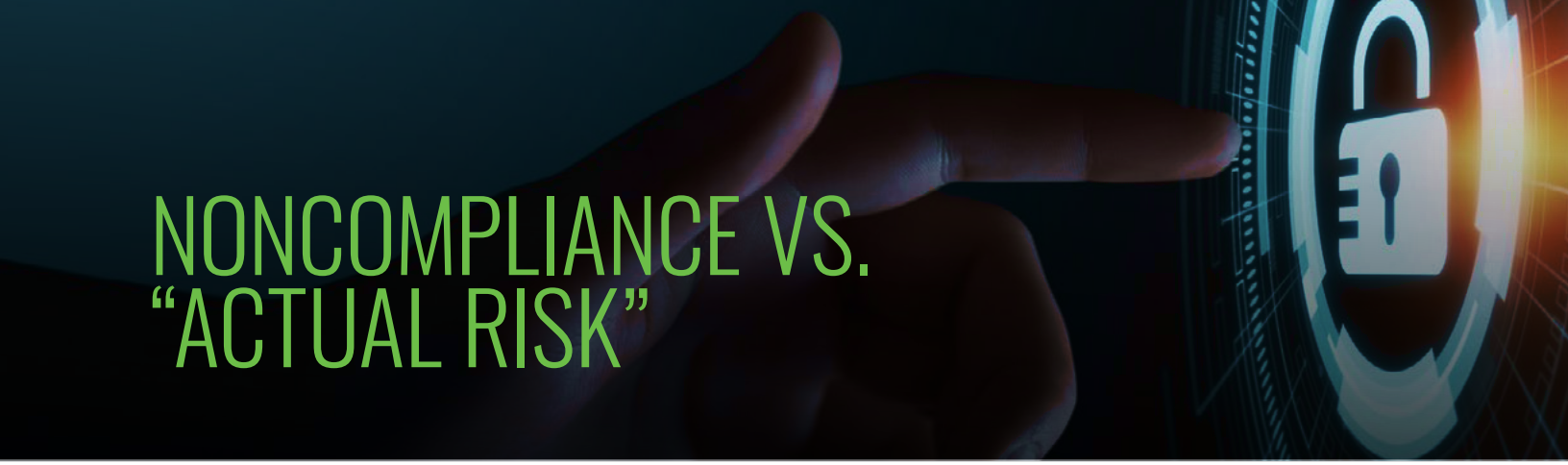


FIGURE 8: FINDING DENSITY ACROSS NONCOMPLIANT PCI-DSS REQUIREMENTS



NONCOMPLIANCE VS. "ACTUAL RISK"

Just as the business criticality of an asset increases the relevance of a noncompliance finding, so does the severity of a flaw, or weakness, that causes a finding. With that in mind, the next step in our analysis is to examine the noncompliance findings against a dimension that may provide a better link between compliance and actual security. To describe that lofty goal of actual security, we'll use a measure that we've used in several previous studies, finding density. Finding density is an organizational metric that takes the number of important findings found on high value assets, divided by the total number of high value assets at the firm. This provides a stable measure to compare large enterprises with smaller organizations.

Looking across all standards, the finding density is relatively uniform. The overall density is displayed below in Figure 9.

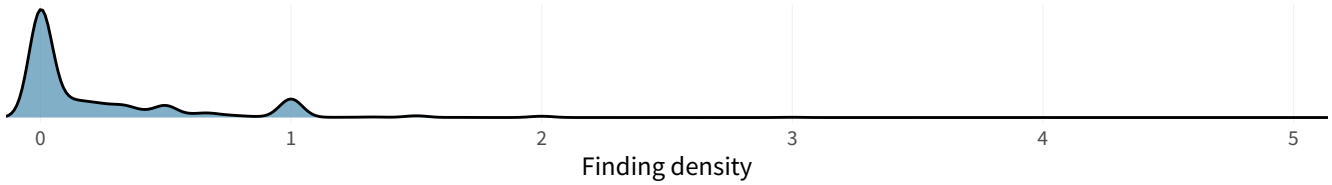


FIGURE 9: RANGES OF FINDING DENSITY FOUND WITHIN ORGANIZATIONS WITH NONCOMPLIANT ITEMS

We get interesting results when we examine the relationship between organizations with compliance-specific issues, and finding density, as seen below.

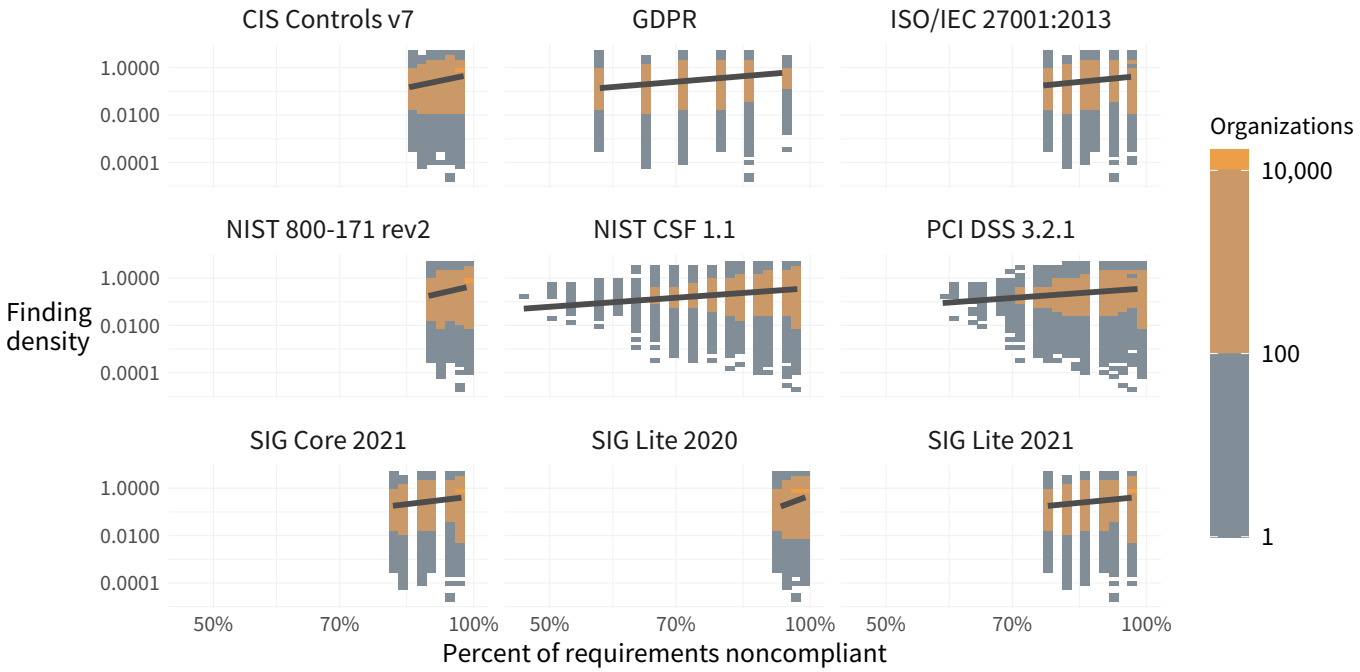


FIGURE 10: RELATIONSHIP BETWEEN COMPLIANCE ISSUES AND FINDING DENSITY

Broadly, as more requirements test as noncompliance there's an upward trend in finding density. Finding density increases with an increase in the percentage of noncompliant items within an organization. Finding density can also offer some insight into which requirements cause the most trouble within each compliance standard. Each standard contains a different hierarchy of requirements, we've simplified this down to each major category of requirements in these standards and show them in Figure 11 below.

FINDING DENSITY:

GREATER DETECTED SECURITY ISSUES PER HOST INDICATES A "DEEPER" LEVEL OF NONCOMPLIANCE

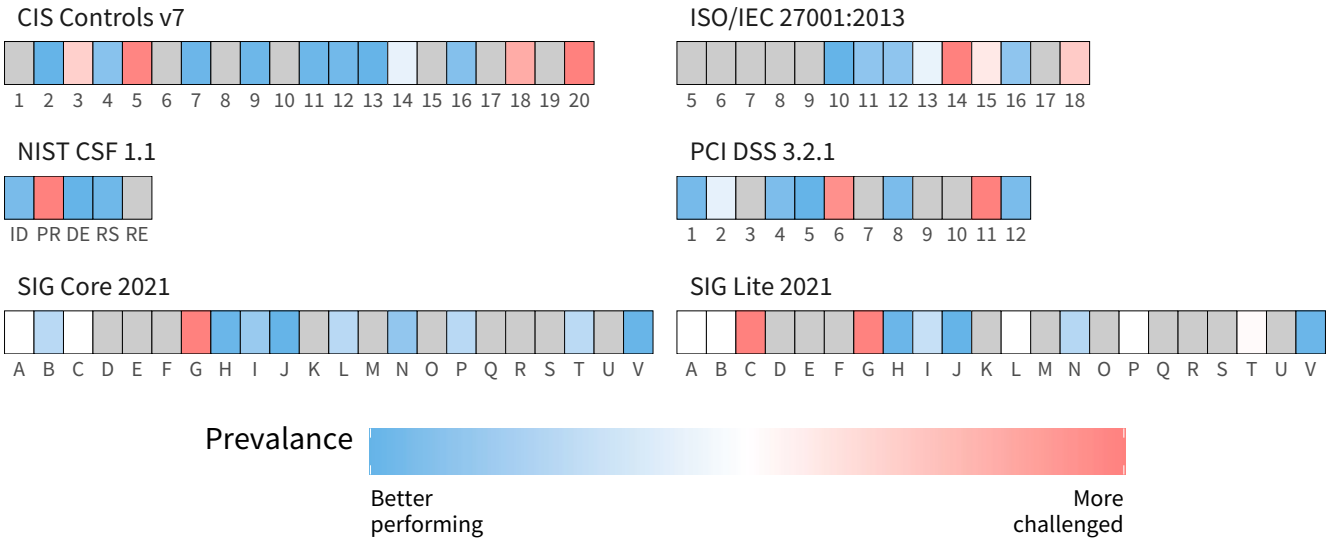


FIGURE 11: DENSITY OF NONCOMPLIANCE ACROSS DIFFERENT REQUIREMENTS

FOCUS AREA:

THE ONE THAT IS MOST CHALLENGING FOR ORGANIZATIONS IS ISO 27001 REQUIREMENT 14, ENSURING THAT INFORMATION SECURITY IS AN INTEGRAL PART OF INFORMATION SYSTEMS ACROSS THE ENTIRE LIFECYCLE.

Now, let's take a look at NIST CSF. The PR (Protect) requirement, with its extensive collection of technical measures (including patch management) seems to be the requirement that presents the most challenges. For the CIS Controls framework requirements 5 (Secure Configuration) and 20 (Penetration Tests and Red Team Exercises), tend to have the most challenges. Hopping down to PCI, it's perhaps no surprise that the technical demanding requirements 6 (Develop and maintain secure systems and applications) and 11 (Test security systems and processes regularly) are the ones that give organizations the most trouble. ISO 27001 requirement 14 (Ensuring that information security is an integral part of information systems across the entire lifecycle) is the one that is most challenging.

IDENTIFYING THE MOST COMMON SECURITY ISSUES CAUSING NONCOMPLIANCE

The security findings discovered in RiskRecon assessments consist of checks of across 40 discrete security criteria that are then grouped into nine generalized security domains. For example, a test of a security control, like the use of HTTP security headers, is a security criteria check. That criterion falls into the overarching security domain of Web Application security, which also includes other criteria, including CMS access control.

FOR THIS REPORT, RISKRECON MAPPED 20 SECURITY CRITERIA AND SEVEN DOMAINS BACK TO THE COMPLIANCE STANDARDS EXAMINED HERE. THESE INCLUDE:

DOMAINS	CRITERIA
DNS SECURITY	DNS HIJACKING PROTECTION
EMAIL SECURITY	EMAIL AUTHENTICATION, EMAIL ENCRYPTION ENABLED
NETWORK FILTERING	IOT DEVICES, UNSAFE NETWORK SERVICES
SOFTWARE PATCHING	PATCHING APP SERVER, PATCHING OPENSSL, PATCHING WEB CMS, PATCHING WEB SERVER
WEB APP SECURITY	CONFIG WEB CMS AUTHENTICATION, WEB HTTP SECURITY HEADERS, UNENCRYPTED SENSITIVE SYSTEMS
WEB ENCRYPTION	WEB ENCRYPTION DATE EXPIRE, WEB ENCRYPTION HASH, WEB ENCRYPTION SUBJECT
SYSTEM REPUTATION	OST HACKING, HOST SCANNING, PHISHING SITE

TABLE 1: DOMAINS AND CRITERIA

Combined Domain and Criteria Problems

Combining our views of common issues across domains and criteria, it's clear how much variability there is amongst all these categories and subcategories.

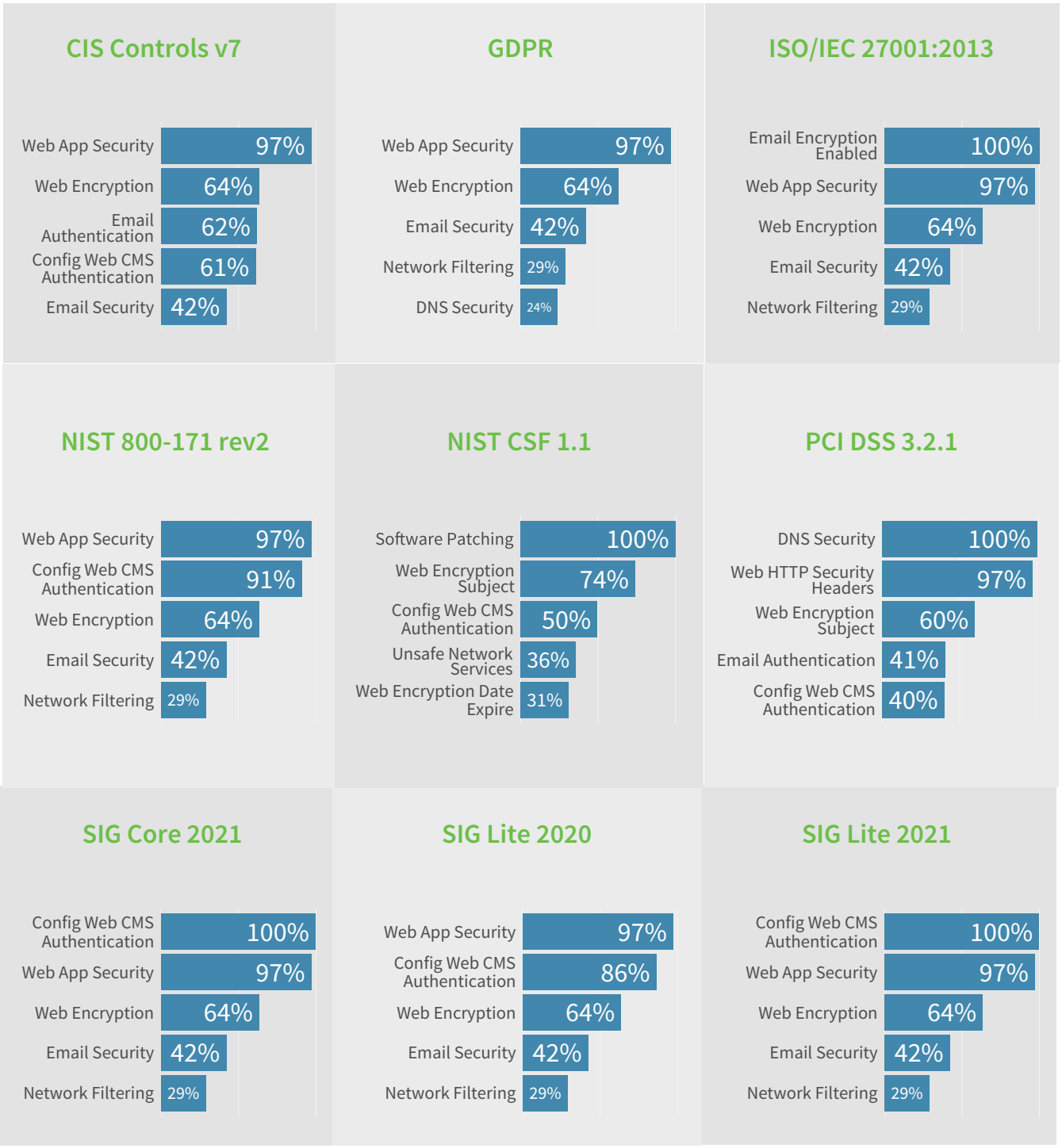


FIGURE 12: TOP FIVE ISSUES FOR EACH STANDARD AND THE PERCENTAGE OF ORGANIZATIONS EXPERIENCING THEM

INDUSTRY SNAPSHOT

What industries struggle most with compliance standards?

ONE OF THE QUESTIONS WE HOPED WE COULD ANSWER WITH THIS ANALYSIS IS: WHAT INDUSTRIES STRUGGLE MOST WITH COMPLIANCE STANDARDS?

Interestingly, when we break our sample up by industry and look at the distribution of noncompliant requirements per organization, the median pattern doesn't vary a great deal across industries. ISO is the most challenging, while NIST CSF is the most compliant.

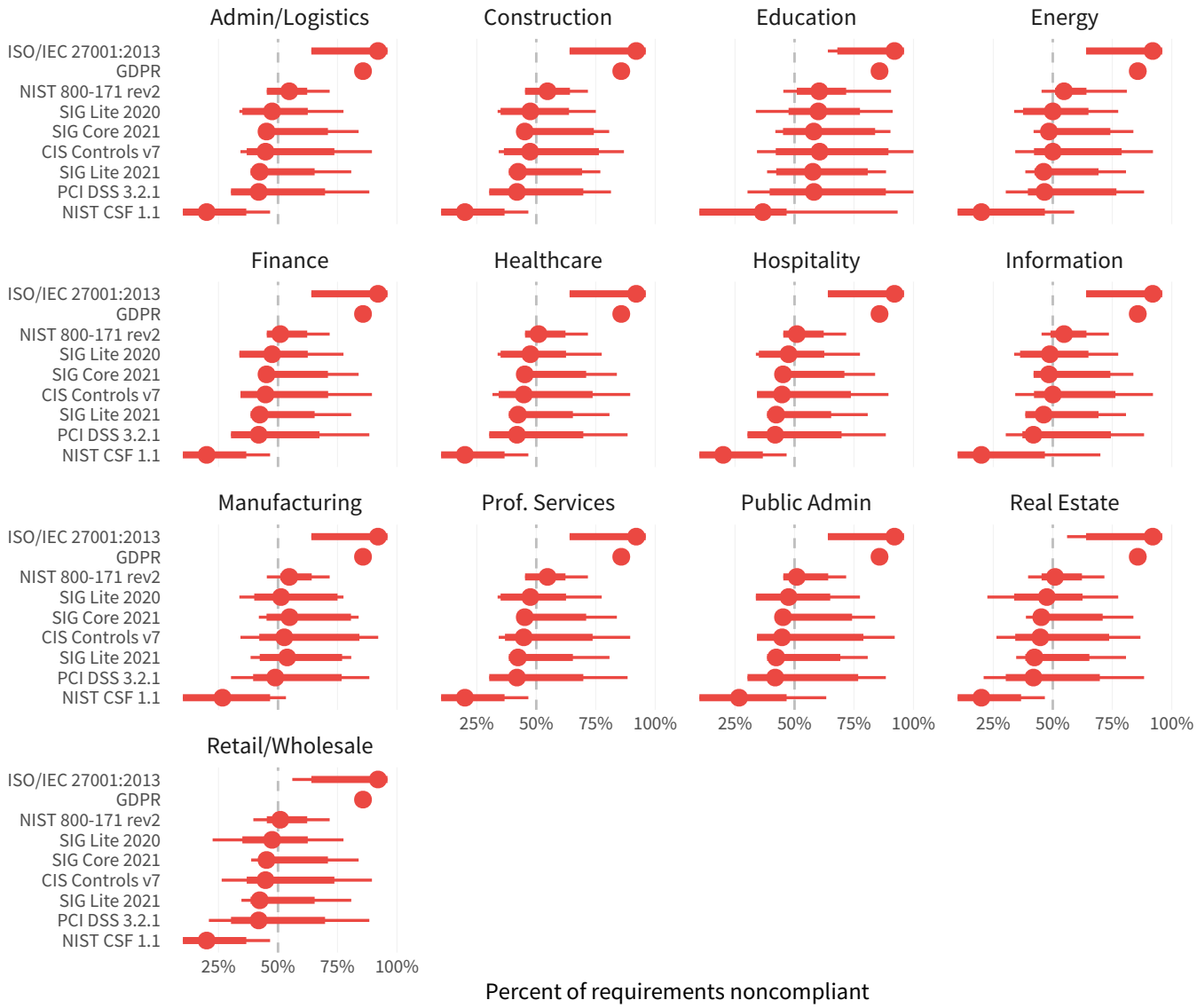


FIGURE 13: DISTRIBUTION OF NONCOMPLIANT REQUIREMENTS PER ORGANIZATION

The box plots show signs of the predictable pattern of Education being the most challenged and Finance emerging as the least challenged. This is a trend we've seen in the past (see previous work such as The Value of Better Data in Third-Party Risk Assessment). However, a better assessment of how well industries are doing is one viewed in light of finding density—as a review, that's the number of compliance findings on high value hosts divided by the total number of high value hosts at organizations.

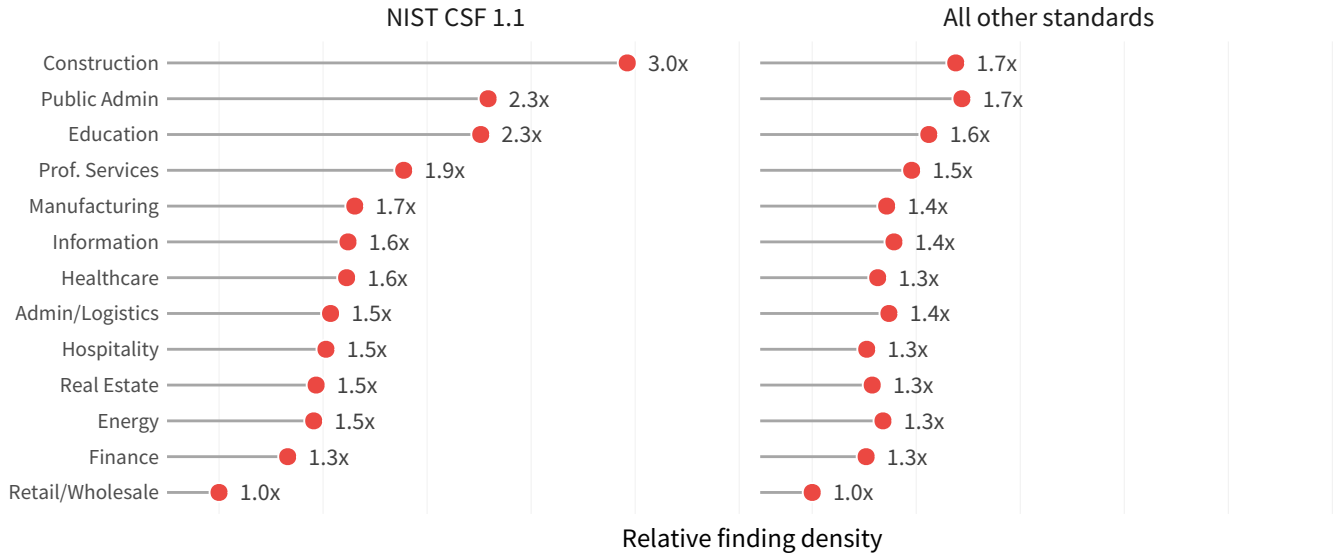


FIGURE 14: RELATIVE FINDING DENSITY ACROSS INDUSTRIES AND STANDARDS

THE INDUSTRIES THAT NEED THE MOST WORK ACROSS ALL STANDARDS ARE:

CONSTRUCTION

PUBLIC ADMINISTRATION

REAL ESTATE

CONCLUSION

Organizations across all industries are tasked with keeping their clients, as well as their own information safe. While compliance does not guarantee security, working to meet compliance standards is a way for many companies to build various security practices into various parts of their organization and business. Cybersecurity regulations and frameworks, authored by a bevy of government and industry oversight groups, can provide a barometer for baseline security best practices. Regardless of whether the standards are coming from the PCI Council, NIST, ISO, or CIS, they can offer an refernce point for organizations can use to chart their security risk posture journey. Even so, almost every single organization has some form of noncompliance.

Throughout this report, we have worked to unpack and understand the risk associated with noncompliance. We found that when an organization's host is in the cloud, that they are also significantly less likely to have compliance issues than organizations with on-premise hosts. When we took a look at noncompliance and how it related to "actual" risk, we looked through our finding density lens to examine the results. We found that finding density increases with an increase in the percentage of noncompliant items within an organization. Even through an industry lens, we didn't see a difference in the median of noncompliant requirements - consistently ISO is the most challenging to meet, while NIST CSF is the most compliant.

FOCUS AREA:

WE FOUND THAT FINDING DENSITY INCREASES WITH AN INCREASE IN THE PERCENTAGE OF NONCOMPLIANT ITEMS WITHIN AN ORGANIZATION. EVEN THROUGH AN INDUSTRY LENS, WE DIDN'T SEE A DIFFERENCE IN THE MEDIAN OF NONCOMPLIANT REQUIREMENTS.

CONSISTENTLY ISO IS THE MOST CHALLENGING TO MEET, WHILE NIST CSF IS THE MOST COMPLIANT.

FOCUS AREA:

COMPLIANCE STANDARDS - AND WORKING TO ACHIEVE THEM - HELP TO MINIMIZE THE AMOUNT OF IMPORTANT FINDINGS FOUND ON HIGH VALUE ASSETS THAT AN ORGANIZATION HAS.

So, what does this mean for organizations looking towards compliance as a measure of security? We know, and understand, that checkbox compliance isn't a path leading to a robust risk management posture. However, we can clearly see that noncompliance does increase the finding density within organizations. While they are not a silver bullet for a risk-free security program, compliance standards - and working to achieve them - do help to minimize the amount of important findings found on high value assets that an organization has.

This is just the beginning of working to understand the relationship between risk posture and noncompliance. The more that continues to be shared across and between organizations and industries, the more likely we will be able to continue to draw correlations and conclusions about the relationship between compliance and risk.

APPENDIX: METHODOLOGY

RiskRecon assessments provide a rich profile of the assets and the details of an enterprise's security configuration and operations. RiskRecon conducts its assessments with no inside access and no initial knowledge of the enterprise being assessed. RiskRecon algorithms automatically discover assets and assess their security operations and configuration quality based on publicly accessible information.

The analysis here is based on anonymized data from thousands of assessments of organizations worldwide. The following figure displays the common indicators pulled from these assessments and how they were mapped back to the included compliance standards.

Indicator	CIS Controls v7	GDPR	ISO/IEC 27001:2013	NIST 800-171 rev2	NIST CSF 1.1	PCI DSS 3.2.1	SIG Core 2021	SIG Lite 2020	SIG Lite 2021
Config Web Cms Authentication	Mixed			Assess	Assess	Mixed	Assess	Assess	Assess
Data Loss	Inform	Assess	Mixed	Assess		Inform	Assess	Mixed	Assess
Data Loss 12					Assess				
Data Loss 24					Assess				
Data Loss 36					Assess				
Data Loss 36 Plus					Assess				
Data Loss 6					Assess				
Dns Security	Mixed	Assess	Assess	Assess		Mixed	Assess	Assess	Assess
Email Authentication	Assess					Mixed			
Email Encryption Enabled	Assess		Mixed	Assess	Assess	Mixed	Inform	Assess	Inform
Email Security	Mixed	Assess	Assess	Assess			Assess	Assess	Assess
Iot Devices					Assess	Mixed	Assess	Assess	Assess
Network Filtering	Mixed	Assess	Assess	Assess			Assess	Assess	Assess
Patching App Server					Assess	Mixed			
Patching Openssl					Assess	Mixed			
Patching Web Cms					Assess	Mixed			
Patching Web Server					Assess	Mixed			
Shared Hosting							Inform		
Software Patching	Mixed	Assess	Assess	Assess	Assess		Mixed	Assess	Mixed
Threat Intell	Mixed	Assess	Inform	Assess	Assess		Assess	Assess	Assess
Threatintel Botnet Host					Assess	Mixed			
Threatintel Cc Server					Assess	Mixed			
Threatintel Hostile Host Hacking					Assess	Mixed			
Threatintel Hostile Host Scanning					Assess	Mixed			
Threatintel Other					Assess	Mixed			
Threatintel Phishing Site					Assess	Mixed			
Unencrypted Sensitive Systems	Mixed							Assess	
Unsafe Network Services	Inform				Assess	Mixed			
Web App Security	Mixed	Assess	Mixed	Assess			Assess	Assess	Assess
Web Encryption	Mixed	Assess	Mixed	Assess			Mixed	Assess	Mixed
Web Encryption Date Expire					Assess	Mixed			
Web Encryption Date Valid					Assess	Mixed			
Web Encryption Hash	Assess				Assess	Mixed			
Web Encryption Key Length					Assess	Mixed			
Web Encryption Protocol					Assess	Mixed			
Web Encryption Subject					Assess	Mixed			
Web Http Security Headers						Mixed			

FIGURE 15: COMMON INDICATORS ACROSS STANDARDS

THE RISKRECON CHECKS IN THIS DATA SET ARE ONLY FOR THE NEGATIVE OUTCOMES.

Note that the RiskRecon checks in this data set are only for the negative outcomes. We have no positive checks that say that "Yes, this asset is likely to be compliant," only that "This asset has potential problems."

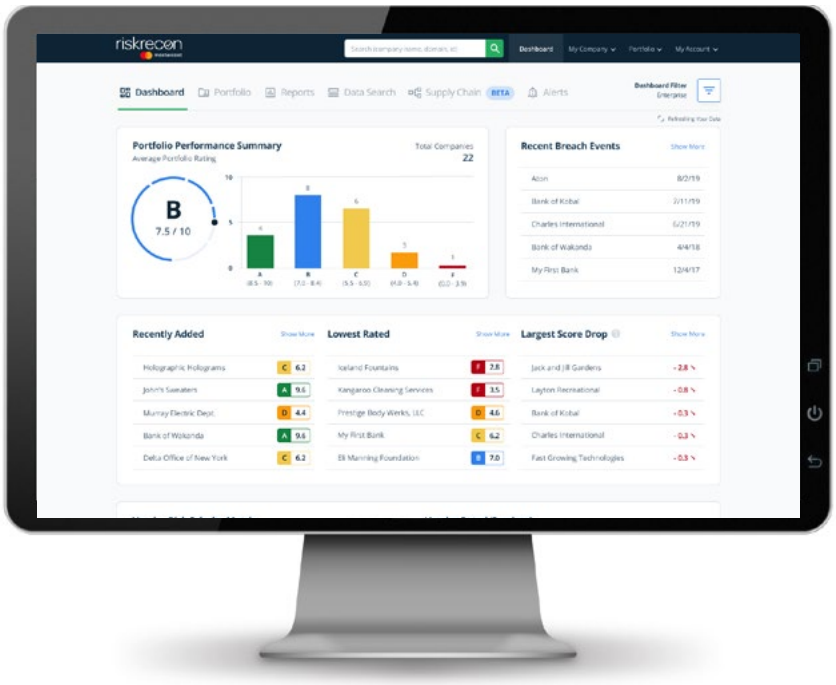
Further, the RiskRecon compliance dashboard (the way these are surfaced in the RiskRecon platform) does not take into account the asset relevance to the standard. In other words, if an asset triggers a check on a PCI requirement, but is not in scope for PCI, RiskRecon cannot determine that remotely. As a result, some things may be over-reported, while internal assets (those not visible to RiskRecon) are under-reported.

FREE OFFER: *KNOW YOUR THIRD PARTY SECURITY RISKS*

As a busy third-party risk professional taking swift action with limited information is no easy feat. Fortunately, RiskRecon is offering complimentary enterprise access to assess and monitor the cybersecurity of your supply chain for 30 days. For 30 days you can enjoy a detailed view of the risk up to 50 vendors pose to your organization. Plus, you'll learn how to use these scores to influence corrective action with risk prioritized data based on issue severity.

WHAT'S INCLUDED IN THE OFFER?

- Detailed assessment of your own IT assets
- Security ratings and summary assessment of up to 50 vendors
- Full access to RiskRecon Technical Support
- A risk-prioritized view into your vendor ecosystem with our vulnerability matrix
- Superior data accuracy (over 99% - which drastically reduces false positives)



REGISTER TO GET INSIGHTS INTO YOUR SUPPLY CHAIN AT https://www.riskrecon.com/know-your-portfolio.

riskrecon

mastercard

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

119 Cyentia INSTITUTE

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com