ARCTIC WOLF

THE STATE OF COMPLIANCE 2022 TRENDS

Table of Contents

01

FOREWORD

Foreword

Within the world of cybersecurity, there are many domains made up of different areas of expertise. There is offensive security for proactive vulnerability identification, incident response for attack management, digital forensics for root cause analysis, and many, many more. It is within these areas of expertise that one domain is often overlooked. It is an area that may not be the most glamorous aspect of cybersecurity, but it is crucial to a successful security program. You may have guessed by the title of this report, but I am talking about those individuals who dedicate themselves to ensuring their organizations meet designated compliance requirements.

Consider the term “compliance” itself and the feelings it evokes. For those individuals who are currently working in an area of cybersecurity, words like “requirements,” “rules,” “violations,” and “fines” come to mind. While these concepts may not carry the same excitement as terms like, "red teams," "blue teams," and "threat hunting," they are an equally important domain in cybersecurity.

Compliance standards are designed to give organizations a foundational approach to designing their security program while also reassuring outside entities that interact with your business that you have met at least a minimal set of security controls set forth by a neutral governing body.

That definition doesn’t do much to increase the excitement around compliance, but let’s rephrase it to better understand. The goal of compliance standards is to let both you and others know that your environment has met a certain level of security standards. In this way, compliance can be seen much like achieving a high school diploma. It denotes to others that you have met the requirements to receive it while also giving you a foundation to continue a lifetime of learning. It may not seem like the most thrilling concept, but it’s the occasionally dull things that keep us healthy that also allow us to be successful and enjoy more exciting endeavors.

Just as a high school diploma is essential to achieving a PhD, meeting compliance requirements is essential to building a successful and trustworthy security program. It is important to also understand that being compliant and being secure are not synonymous. Compliance should be seen as one essential element of a security journey that will last the lifetime of your organization.

The importance of compliance, and the unfortunate way it is sometimes overlooked, is the reason Arctic Wolf chose to invest time into researching current trends in cybersecurity compliance and frameworks. Our research consisted of a series of questions and interviews with 235 North American organizations. In designing our research group, we chose to include all environments of varying sizes, business verticals, and architectural design. This allows us to get a better understanding of the challenges facing a wide variety of businesses and their efforts to achieve compliance. Included in this report are the results of our research and our analysis of the trends we have identified.

It is our hope that this report helps organizations better understand both the challenges and successes others are facing as we strive to achieve our goal of Ending Cyber Risk.

Christopher Fielder
Field CTO – Arctic Wolf

01

02

CURRENT STATE OF CYBERSECURITY COMPLIANCE

A Compliance & Standards Usage

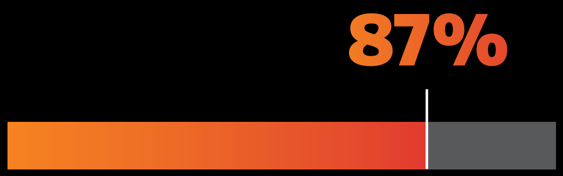
B Current Compliance Trends

C Determining Requirements

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Compliance & Standards Usage

Because creating a successful cybersecurity program can be a difficult, complex task, many organizations have chosen to follow a predefined framework or set of compliance guidelines to both establish and improve their programs.



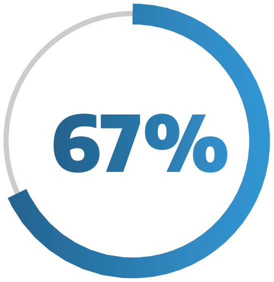
In our research, we found that 87% of organizations currently adhere to some form of cybersecurity compliance standards or framework.

02A

Protecting an organization from cyber threats and the myriad of cyber incident scenarios can feel overwhelming, and many businesses struggle to find a starting point.

Compliance requirements, or a security framework, can be an excellent resource for security teams and guide them as they build out their program.

However, even knowing which requirements to follow can become an arduous task since compliance is dictated by different aspects of an organization's business.



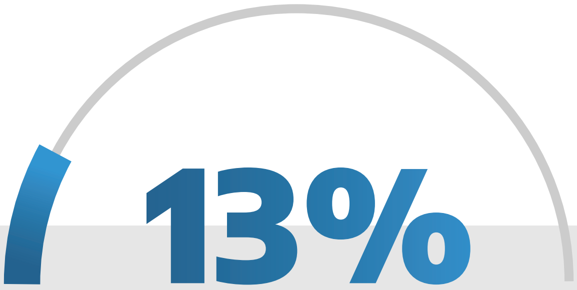
We identified that 67% of our respondents follow between one to three sets of guidelines, with those following less sets of standards finding it easier to maintain compliance.

The simplistic approach of a single set of standards isn't an option for all organizations. Six percent of the businesses we researched are required to follow six or more sets of compliance and framework standards. This can be challenging when we consider how increasing the number of compliance standards also increases the difficulty of meeting all their requirements.

To add further complexity to this is the way competing standards may have varying degrees of rigor to achieve compliance. When faced with this challenge, Arctic Wolf recommends following the most detailed and strict requirements from each standard to ensure compliance is met.

Compliance & Standards Usage

Deciding which compliance frameworks to follow, or whether to follow any at all, varies by industry and organization size.



Thirteen percent (13%) of respondents to our survey stated their organizations do not currently follow any form of compliance or framework guidance.

This could be due to several factors outside of just willingly choosing to ignore compliance. Smaller organizations, such as SMBs, don't yet have the resources to focus in detail on compliance, or it is yet to be part of their business plan. It's also possible that, due to specific business needs, some organizations have chosen to forge their own path and develop their cybersecurity program without the aid of a predefined framework. This is entirely possible in verticals such as tourism, retail, wholesale, and entertainment. Those verticals have less stringent compliance standards as compared to highly regulated industries like healthcare and finance, especially so for SMBs or even startups.

While compliance may not be on the forefront of certain organization's minds, especially if they are just starting out, compliance can help a business achieve a strong cybersecurity posture. Every business, regardless of size, industry, or business goals, should be diligent about following any regulatory requirements to protect both their organization and their clients or customers.

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Current Compliance Trends

Identifying which compliance standards your organization is obligated to follow, or which cybersecurity framework best fits your unique environment can be a challenge when we consider the number of options that are currently in use. To understand this better, we should consider the results of our research.

02B

Organizations are suffering from a plethora of choice when it comes to picking and implementing a compliance framework. The number of options has multiplied over the years.

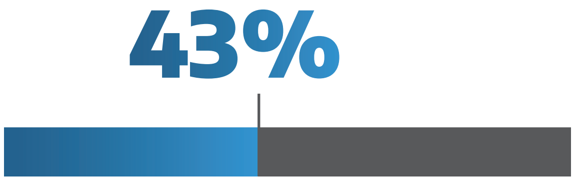
While Arctic Wolf's survey asked respondents to choose from the 12 most common standards currently in use, 16% of respondents stated they follow additional standards outside of the 12 we included.

Lesser-known standards can present both a benefit and a challenge to companies depending upon the situation. Less common frameworks can be specifically designed to tackle the challenges of unique business needs and therefore, allow an organization to hone in on their exact security requirements.

For example, many financial institutions may be required to adhere to FFIEC requirements while some financial institutions within New York must also comply with the New York Department of Financial Services (NYDFS) Cybersecurity Regulation. However, other organizations may be unaware of a lesser utilized standard and therefore overlook their obligation to meet these requirements.

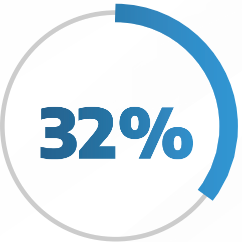
Current Compliance Trends

Conversely, we found that the most common compliance standards being adhered to is the Health Insurance Portability and Accountability Act, or HIPAA.



Forty-three percent (43%) of organizations are required to meet HIPAA compliance standards to ensure they are actively taking measures to protect the sensitive patient health information of their customers.

This may appear initially to be a high percentage, but it is important to note that there is a misconception that HIPAA compliance is only focused on the healthcare sector. Instead, any entity that processes, manages, or maintains personal health information (PHI) must comply with HIPAA. When we consider how often an individual's PHI may be utilized it becomes clear why so many businesses must meet HIPAA compliance.



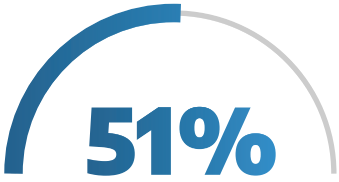
The second most used compliance standard we found was the Payment Card Industry Data Security Standard, or PCI DSS, with 32%.

PCI is designed to ensure businesses that accept and process payments from the major credit card providers are meeting a minimum set of security standards to protect credit card data. The frequency of these two seemingly different compliance standards highlights our previous point on the need for many organizations to follow multiple compliance standards focused on different security goals.

Consider a pharmacy: Where a pharmacy business must meet HIPAA compliance due to their handling of patient records, they must also comply with PCI guidelines if they accept credit card payments for their services. We could also consider what it would mean if our example pharmacy was also a publicly traded company. In this situation they would also be required to comply with Sarbanes-Oxley Act (SOX) standards. Compliance standards can quickly mount and multiply.

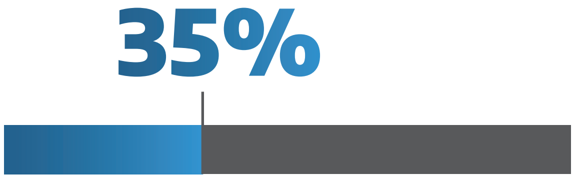
Current Compliance Trends

Supplemental framework adoption is expanding beyond just industry requirements, however. They are also setting the standard for building out a security program.



Fifty-one percent (51%) use the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

This popular framework was designed to assist organizations in assessing their security risk. The NIST Framework defines the five cybersecurity functions of Identify, Protect, Detect, Respond, and Recover and further breaks these down into 23 categories and 108 subcategories that allows organizations to methodically work through the framework. Anecdotally, we have heard from some of our respondents that they find this framework attractive due to its comprehensive approach and structure.



Our research also showed 35% of our participants use the Center for Internet Security (CIS) Controls as a guiding framework, making it the second most popular framework overall.

Currently published as Version 8, these controls detail recommended actions to ensure strong cyber defenses, including information on how to prevent commonly known attacks. The popularity of both NIST and CIS Controls highlights the layered approach organizations are taking when it comes to utilizing frameworks. Security conscious organizations are choosing to follow multiple frameworks as a method of minimizing gaps in their security posture.

CURRENT STATE OF CYBERSECURITY COMPLIANCE

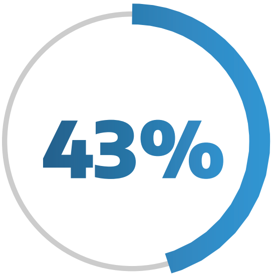
Determining Compliance Requirements

Before an organization begins the process of conforming their cybersecurity program to an existing framework or working towards achieving compliance, it must take the initial step of determining which set(s) of standards to follow.

02c

This process ensures an organization is working towards meeting the correct set of requirements without the undue burden of following guidelines that may be unnecessary. Identifying which compliance standards a company must follow, however, is not always as simplistic as it may seem. As outlined in our previous example, some organizations may find themselves obligated to follow multiple disparate compliance standards. In the worst cases this could result in a business failing to meet compliance requirements they were unaware of.

Almost half of all organizations are forgoing that process all together.



Forty-three percent (43%) of organizations admit to following their compliance requirements solely due to the legal obligation to do so.

In these cases, the business may have chosen a set of standards that only meets required standards, without considering what is best for their security environment. While this is an understandable situation, security and compliance go hand in hand, so it's imperative that organizations meet both legal requirements and frameworks that best fit their overall security needs. Achieving a state of compliance is important when it is required, but it is equally important to ensure that compliance steps map directly to true risk mitigation for your organization.

Determining Compliance Requirements

Business factors aren't the only drivers of compliance. We found that 16% of respondents follow guidelines or standards based on the requirements of outside business factors.

This can include both compliance and frameworks set forth by customers or vendors. Let's consider the importance of this within the context of modern cyber threats. A recent statistic shows a 300% increase in software supply chain compromises from 2020-2021. As a result, organizations must not only ensure they are protected from compromised vendors, but also shield themselves from being the entry vector by which their customers are compromised.

19%

A concerning trend we found, considering the above, was that 19% of organizations admit to being unsure of why they follow their current compliance standards.

Our research found that many of these organizations follow their established standards with a "business as usual" mindset. This is one where their security program is designed to meet the established requirements simply because that's the way they've always done it.

As the cybersecurity landscape evolves, these organizations are setting themselves up for future security failures. An organization's security posture should be seen as a continual journey of improvement. One that grows, matures, and evolves with the company. If a business follows a static set of requirements without an understanding of why they are attempting to meet these guidelines, they risk outgrowing their prescribed set of standards.

A symptom of outgrowing such standards would be ignoring the evolution of your environment's architecture regarding your security standards. Perhaps you have expanded your business to include innovative technology and cloud resources, yet your compliance standards aren't updated to reflect these new features. This results in a false sense of security as an organization meets outdated goals that they have since outgrown. Organizations should regularly reevaluate the goals of your security program and research your compliance obligations.

03

COMPLIANCE TEAMS

A Impact of Dedicated Headcount

B Impact of Budget

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Impact of Dedicated Headcount

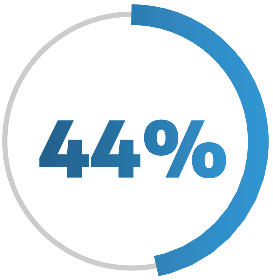
Once an organization has determined which cybersecurity framework and set of compliance standards are correct for their environment, they must then begin the task of implementing these guidelines and monitoring for compliance. This can be achieved in different ways.

Our results found that only 32% of organizations have a team that consists of multiple individuals that are dedicated to ensuring compliance is met.

These teams generally fall under the direction of a CIO or CISO, work within a larger Information Security team, and have a separate compliance-focused budget Those 32% also feel confident in their team, noting that their organization falls into the “very compliant” category.

03A

Not all organizations have the means to develop a dedicated compliance team, however.

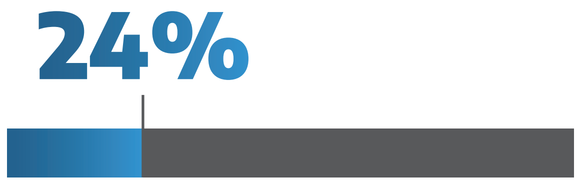


We identified that 44% of our responses classified themselves as having one or more individuals within the larger information technology group who is tasked with dedicating their time to ensuring the organization remains within compliance standards.

This individual may not have the resources of a full compliance team or similar budget, but their time is devoted to ensuring compliance is met. These organizations also maintain an elevated level of confidence that they are compliant.

A Impact of Dedicated Headcount

The confidence an organization has that they are within compliance standards drastically decreased for those businesses that are unable to dedicate any of their team members to this function full time.



We identified that 24% of organizations, almost a quarter of our responses, acknowledge the importance of compliance, but find themselves in a position where they are unable to devote any of their employees to focus solely on this task.

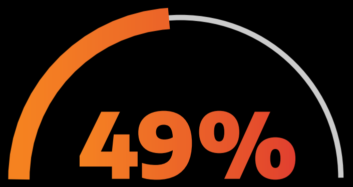
These respondents admitted that their approach to compliance falls under the concept of "best attempt" as they struggle to maintain the necessary talent and resources required to achieve their desired level of compliance success. It was within these responses that we identified organizations that admitted to suffering attacks and paying fines related to compliance failures within the last calendar year.

This is not to say that these businesses are not working tirelessly to ensure the security of their environment, but instead they are often faced with the almost insurmountable task of trying to meet complex compliance standards with limited resources.

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Impact of Budget

Budget is a key factor in developing a successful compliance program and one of the primary reasons a company may point to for their inability to meet required standards.



Our results show 49% of organizations say their biggest hurdle to keeping their environment compliant is rooted in budgetary constraints.

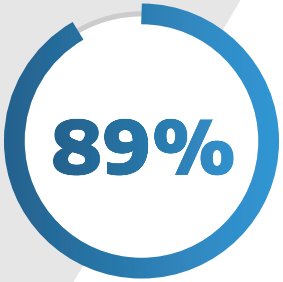
These businesses report that the shortage of necessary funds results in their lack of dedicated headcount and limited resources they would need to maintain compliance.

03B

The cybersecurity skills gap is a concern felt throughout all areas of the information security world.

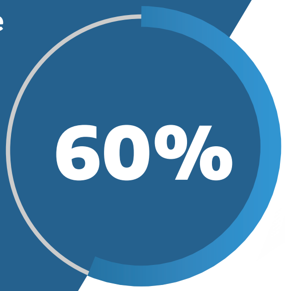
A lack of skilled security experts results in higher salary requirements that may be out of reach for many organizations. In our Arctic Wolf 2022 Security Trends report we found that 76% of organizations identified their inability to staff required functions as their primary obstacle in achieving their overalls security goals. This directly correlates with the struggles we are seeing many companies face with meeting their compliance goals. Many companies are finding that the difficulty in obtaining necessary budget is coming from an increase in talent and technology costs, not from a lack of leadership support.

We found that 89% have received successful buy-in from senior leadership related to compliance. Unfortunately, in many situations this buy-in does not mean an automatic allocation of funding needed to enhance a compliance program.



03B Impact of Budget

Although most organizations agree that achieving their compliance goals requires the necessary funding, 60% of companies spend less than 10% of their overall cybersecurity budget on compliance and risk governance.



Anecdotally we have heard from some respondents that see compliance as a “best attempt” situation. So much so that they include estimated compliance fines in their security budget. This can be overcome if businesses are able to reassess how they spend their cybersecurity.

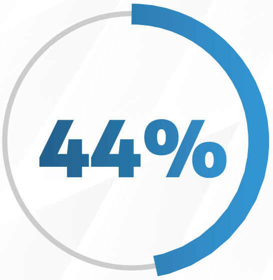
Ninety-seven percent (97%) of organizations plan to spend the same or more on their compliance program in the next year.

Thankfully, organizations are planning for this shift.

Companies that fall under budgetary constraints and struggle to meet compliance requirements should consider the process of running gap assessments. This would allow them to identify areas of non-compliance before they are found to be violations by a governing body that would result in fines or compliance failures.

A gap assessment can be thought of as a compliance practice run. The organization’s security program is informally compared to the set of compliance requirements to determine any areas that do not meet the defined standards. This can be done either by an employee of the company or third-party consulting services that provide an outside perspective.

Despite the importance of a gap assessment in helping to identify areas of non-compliance so they can be remediated, we found that 44% of organizations do not run gap assessments as part of their compliance program or risk management program.



04

ADDITIONAL COMPLIANCE TRENDS: TECH STACK

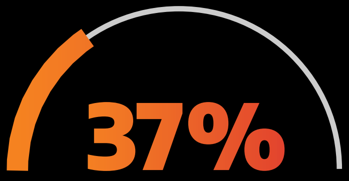
A Lacking System Log Retention and Analysis

B Over Reliant on Firewalls

C Insufficient Incident Response Planning

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Lacking System Log Retention & Analysis



Regarding cybersecurity technology and architecture, 37% of respondents said their organizations do not regularly retain and review system logs as a means of risk monitoring and compliance maintenance.

04A

Systems logs are an invaluable element of visibility into a business's infrastructure and an important part of a compliance program.

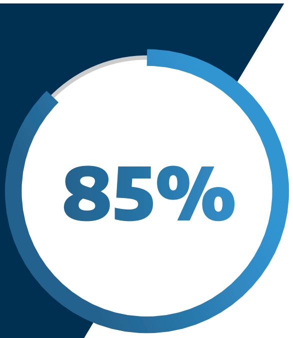
These logs can give detailed information about what is occurring on critical business systems and allow for additional auditing to ensure compliance standards are being met. You can't deter cyber risk if you can't see where that risk is. Furthermore, certain compliance standards such as the aforementioned PCI DSS include requirements for retaining and analyzing event logs for malicious activity. Failure to retain system logs within an environment that processes credit cards would be seen as a compliance violation.

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Over Reliant on Firewalls

In the 2021 Arctic Wolf Security Trends Report we detailed how many organizations still take a legacy approach of considering their firewalls to be the foundational technology of their cybersecurity program. This trend continues according to the results of our compliance research.

We found that 85% of organizations implement a network firewall as the core component they use to maintain compliance and monitor risk.



Firewalls are a principal element of a cybersecurity technology stack, but with a vast array of powerful cybersecurity technology we encourage organizations to consider a balanced approach to designing their technology stack based on what tools and devices work best for their environment rather than simply focusing on firewalls due to their history as a core piece of technology.

04B

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

Insufficient Incident Response Planning

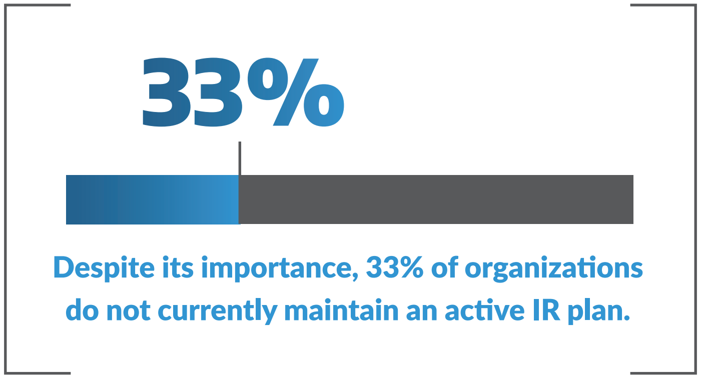
Most of the commonly used frameworks and compliance regulations go beyond firewalls and require businesses to establish an active incident response (IR) plan as a means of mitigating the impact of a cyber attack.

04c

This can be seen as a good guideline for all organizations as an IR plan allows companies to practice incident response drills while refining their process to further reduce the effects of an incident.

Organizations of all sizes should develop and maintain an IR plan so they can quickly respond if or when an event occurs.

Arctic Wolf would recommend all organizations of any size to develop and maintain an IR plan so they can quickly respond when an event occurs.



Despite its importance, 33% of organizations do not currently maintain an active IR plan.

Not only will this result in a compliance violation when an organization's standards require such a plan, but it also leaves organizations scrambling to define the important "who," "what," and "when" of a response scenario as it is occurring. Confusion, delays, and cost can all increase in this instance.

05

ACHIEVING COMPLIANCE SUCCESS

How Arctic Wolf Can Help

CURRENT STATE OF
CYBERSECURITY COMPLIANCE

How Arctic Wolf Can Help

While compliance and security are not one in the same – and meeting a compliance standard should not be conflated with being secure, **compliance initiatives can be an invaluable springboard to propel your organization's security journey forward.**

To reap the posture hardening benefits that compliance frameworks can provide, organizations need to identify which cybersecurity framework and set of compliance standards are correct for their environment, then they must start the process of implementing these guidelines and monitoring for compliance.

If there are challenges that stand in the way of meeting your compliance goals – whether that be limited budget or headcount, or lack of internal expertise, Arctic Wolf can help by providing:

- Guidance across every step of your compliance journey—from planning to implementation to audit assistance
- Deep knowledge of compliance requirements across industries and geographies
- Proactive 24x7 threat monitoring, rapid response, and remediation to prevent potential incidents before they become breaches
- Strategic reviews to optimize your organization's ability to document and demonstrate compliance activities through custom reports, analytics, and live dashboards
- Log investigation and analysis to deepen visibility into your environment and its unique risks and vulnerabilities
- Custom detection rule creation to ensure adherence to your organization's compliance requirements and security needs

About Arctic Wolf

Arctic Wolf® is a global leader in security operations, delivering a premier cloud-native security operations platform designed to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes more than two trillion security events a week across the globe, helping enable critical outcomes for security use cases and optimizing customers' disparate security solutions. The Arctic Wolf® Security Operations Cloud delivers automated threat detection and response at scale, and empowers organizations of virtually any size to establish world-class security operations with the push of a button.

For more information, visit arcticwolf.com.