THE 2020 STATE OF COMPLIANCE AND SECURITY TESTING REPORT

Synack®

Table of Contents

Executive Summary

The 2020 State of Compliance and Security Testing Report includes data from over 311 organizations across a broad range of industry verticals. It provides some conclusions on 2020 imperatives of security teams including program structure and ownership, compliance requirements, testing approach and vendor strategy. Respondents were drawn from a range of business functions including executives, technology, security and compliance.

It is clear organizations widely utilize third party vendors to support their security and compliance testing goals with over 43% of respondents utilizing vendors in the last 2 years. However 27% of organizations are dissatisfied with the operational process required for managing and scheduling testers, as well as the quality and time spent testing. Alarmingly, 40% of organizations are only spending 8 hours or less of testing per test which can only provide a cursory evaluation of the security posture of the target and will no doubt leave security vulnerabilities undiscovered.

A more positive sign of organizations adapting to meet the evolving and dynamic threat landscape is that 44% of respondents reported performing testing monthly or more frequently. Whilst we would like to see this figure much higher, it is above the typical minimum compliance expectation of annual or quarterly testing. This is no doubt in part being driven by changes in application development practices where Agile and DevOps methodologies are pushing code to production much more frequently. It was interesting to note that 18% of organizations surveyed are enabling their developers to undertake testing in efforts to “shift left” and reduce last minute roadblocks to code release and to take advantage of the cost saving benefits of finding bugs early in the development lifecycle.

32% of respondents considered compliance and security testing as expensive and difficult to scale. Whether slowing down development processes or being challenged to provide security assurance coverage across a large number of assets, the perceived return on Investment for traditional security testing is often low. New and novel approaches are required that address these long standing challenges in the compliance and security testing space.

8% of our Enterprise respondents reported they are beginning to adopt Crowdsourced Security Testing methods to address the compliance testing challenges reported. However it is vitally important to recognize that not all Crowdsourced Security Testing is equal and some delivery methods may introduce more risk than they remove. It is important in your 2020 planning to select vendors that utilize trusted and highly vetted researchers, where testing is performed in a rigorous and structured way to provide test coverage and where endpoint control and operational security controls are a standard, embedded part of the delivery process.

We want to thank the participants of the survey who took the time to answer questions to inform our analysis on compliance and security testing.

Key Findings

The findings from this report tell a story about how today's organizations view security, how they implement compliance testing, and where security practices have room to grow. While every organization surveyed did show a sufficient baseline for security testing, there were trends that appeared that highlight some of the specific challenges and issues that security organizations face today.

60% Compliance and security testing that is designated to departments and roles outside of the security function.

27% Organizations that are dissatisfied with the time and effort required to manage testers and scheduling.

2.7 While organizations often rotate through multiple testing vendors, this is the average number of security testing vendors employed by organizations.

40% Organizations spending fewer than 8 hours hours of testing per each security test.

32% Compliance testing processes are expensive and difficult to scale.

43% Organizations that utilize external security testing vendors to perform their compliance and security testing.

18% Organizations enabling developers to perform security testing within the SDLC.

8% Organizations utilizing Crowdsourced Security including Crowdsourced Penetration Testing and bug bounty to enhance their testing program.

44% Organizations that perform testing once a month or more frequently.

52% Organizations that experience increased cost and complexity due to overlap in functionality from using multiple vendors.

State of Compliance & Security Testing Survey Data Analysis

A Bird's Eye View on Security in Organizations

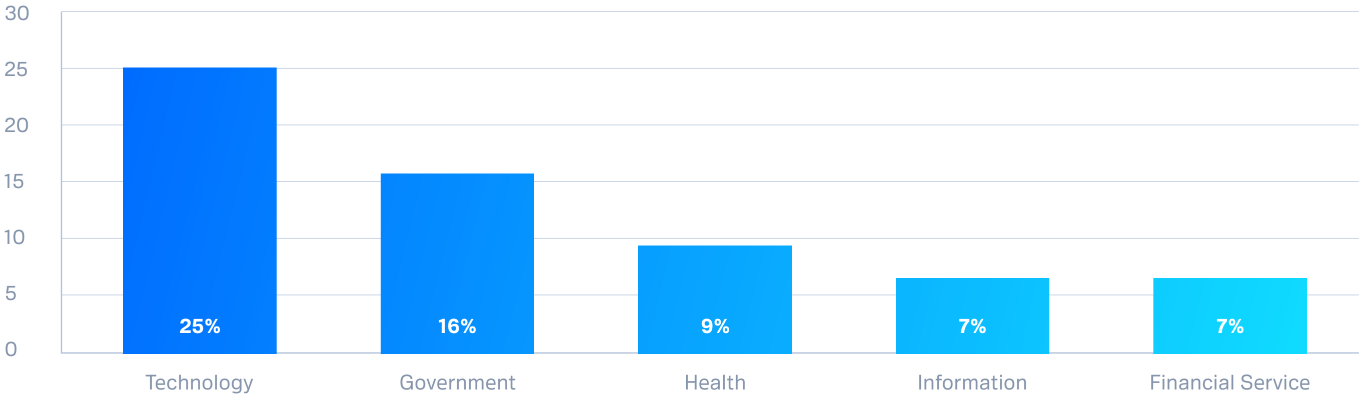
As citizens, employees, customers and consumers we increasing rely upon and utilize technology, from banking, pensions and insurance through to healthcare, tax, travel and transport. The information we share online with the government and service providers is rich and sensitive and is increasingly a target for attack by criminals, malicious nation states and other disruptive groups.

In the face of this, organizations are under tremendous pressure to protect customers' personal data. Organizations need to meet the growing expectations of their executive leadership and shareholders, as well as adhering to the growing number of compliance standards that have been developed to help companies and governments better protect and defend themselves from attacks and breaches. We surveyed over 300 leaders to learn more about security testing and compliance at their organization.

Demographics

More than 311 organizations across North America participated in this year's report from a broad range of industry verticals. Most heavily represented was Technology (25%), Government (16%) along with Health (9%), Information Technology (9%), and Financial Services (8%).

FIGURE 1: The percentage of participating organizations by industry vertical, excluding those contributing less than 1 percent.



> *More than 311 organizations across North America participated in this year's report from a broad range of industry verticals.*

Organization size was evenly represented with approximately a third split across Large Enterprises (1000+ personnel) at 37%, mid-size companies (100-999) at 28% and small companies (1-99) at 35%.

Individual respondents classified themselves into organization functions and roles and were mostly comprised of Information Technology (45%), Executives (20%) and Security (10%) with Development and Product Management comprising a further 15% combined.

FIGURE 2:
The percentage of organizations by size (personnel)

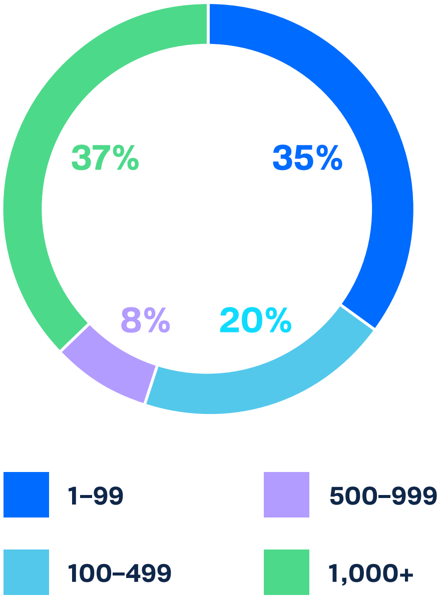
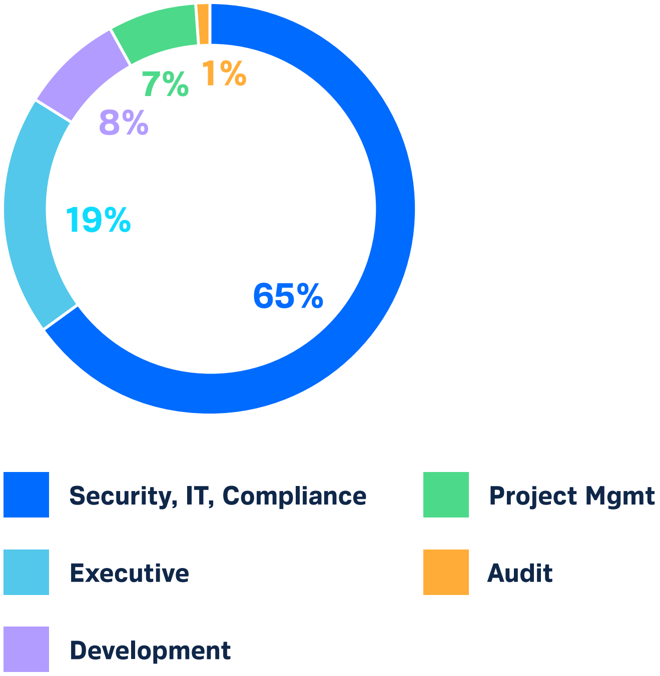


FIGURE 3:
The percentage of respondents by role/function



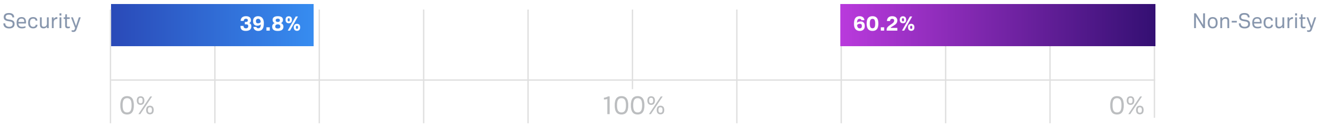
Deconstructing Compliance Security Testing

What department or individual owns day-to-day compliance testing in your organization?

It is useful to understand which function in an organization has accountability for the organization's compliance security testing. In business, compliance refers to obeying all relevant laws and regulations, internal standards and practices. Compliance is typically a business accountability, but where regulations apply to technology and data, IT and Security leadership have a significant role to play, taking varying levels of accountability and responsibility dependant on organisation size and structure.

Respondents indicated that IT related functions and roles (CTO, CIO, Other IT) were most common in taking day to day ownership of compliance testing at 43% with Security functions (CISO, Security) closely following at 40%.

FIGURE 4: Security versus Non-Security roles in terms of who owns the organization's compliance testing.



This result is likely reflective of compliance being a business concern with IT accountable for undertaking such duties extending to testing. It could also reflect organizational structure and reporting lines with the CISO reporting to the CIO who ultimately is accountable. Company vertical and size also plays a role as small and mid-size companies typically have smaller security teams often without a dedicated CISO that reports up through IT.

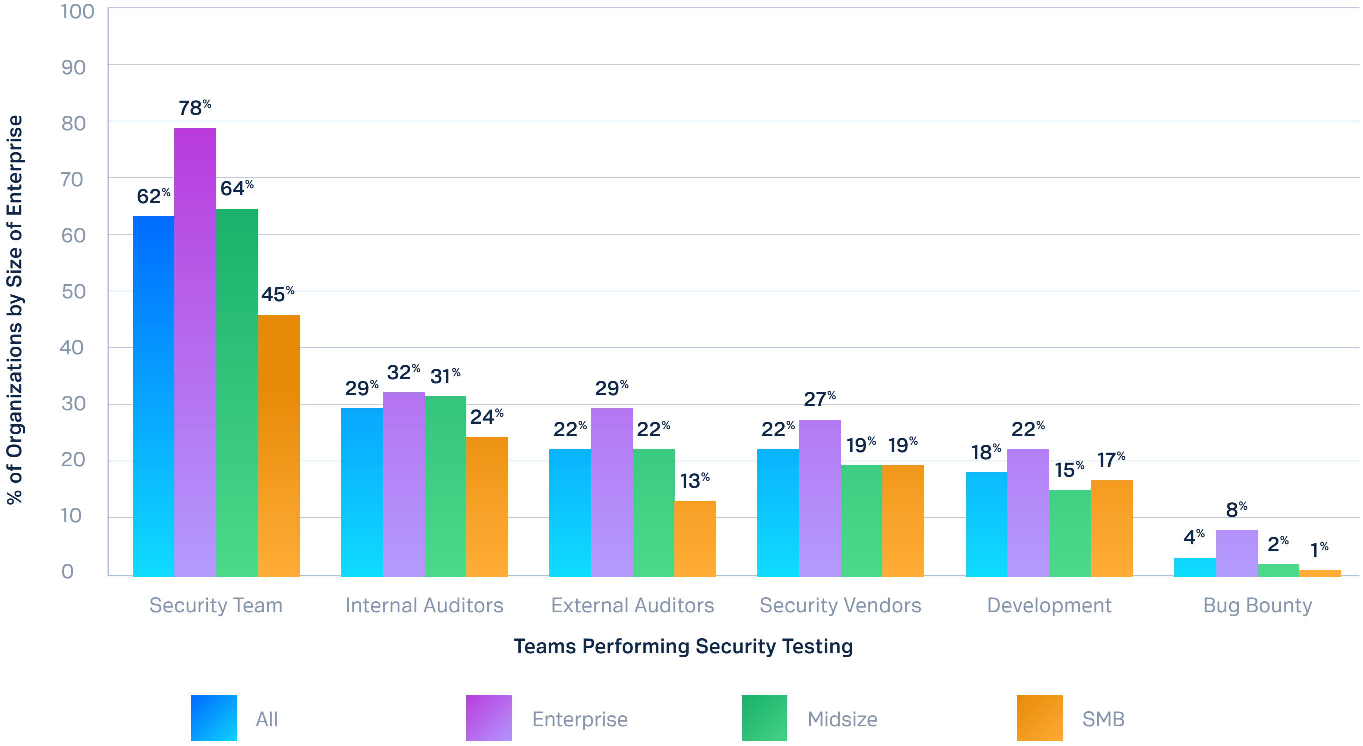
Often testing programs are centrally structured and operate under a delegated model to ease budget and operational challenges given a large attack surface and a small central security team. However, there are significant security benefits to a more centralized security testing program including test quality, control, risk reporting and visibility.

> “*Respondents indicated that IT related functions and roles (CTO, CIO, Other IT) were most common in taking day to day ownership of compliance testing at 43% with Security functions (CISO, Security) closely following at 40%.*

Who performs your security testing?

It was clear when asking respondents to indicate who performs security testing in their organization that overwhelmingly this was their Security Team (59%). Ideally, vendors are used to help scale and provide a 3rd party perspective. As you can see in the breakdown by organization size, Enterprise organizations utilize internal security teams, external auditors, and security testing vendors more than midsize and SMB organizations. This is likely due to the larger attack surfaces and therefore budgets required to help mitigate the risks faced and the increased regulation and compliance demands.

FIGURE 5: Who performs security testing by organization size



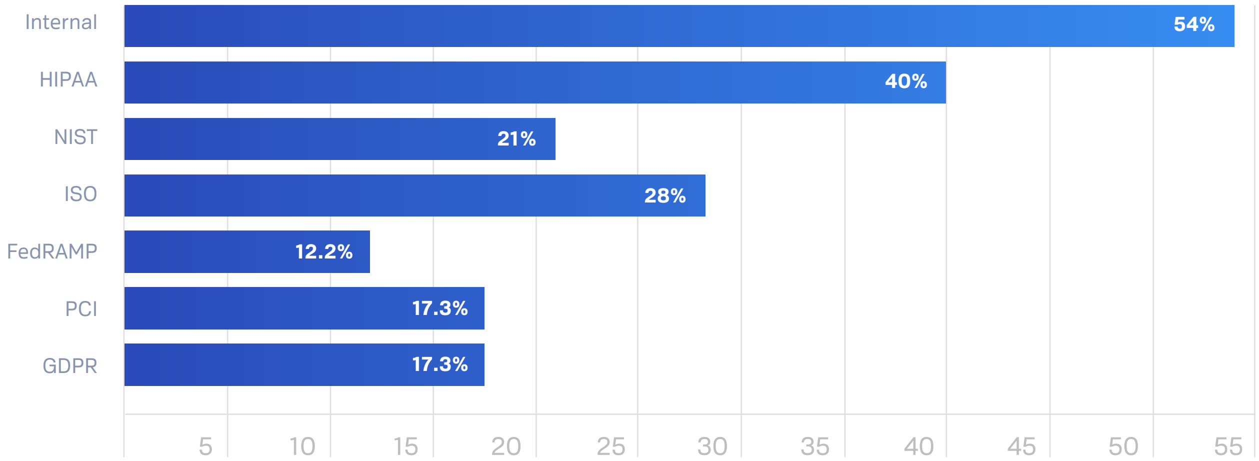
Interestingly 18% of organizations permit their developers to perform security testing following the continued trend of “shifting left” in the development process to help find security bugs as early as possible to reduce remediation costs. This should not replace an independent security check but is a beneficial compliment to help improve secure coding practices and improve security at the source.

Finally of note was the fact Enterprise are more likely to employ a Crowdsourced Security Testing approach than small and medium size businesses. This may be due to the additional assurance gained by complimenting penetration testing and Bug Bounty approaches where the incentivized nature and unstructured method of a Bug Bounty supports the structure and coverage of a penetration test. With the further development of Crowdsourced Penetration Testing, there is an approach that offers the advantages of both combined.

Which compliance and best practice standards are you adhering to or striving for?

There are a large and increasing number of security compliance standards that organizations need to adhere to. These are often dictated by the company industry vertical or the type of information being processed. What initially stood out was that 54% of respondents had internal company standards that had to be complied with. Perhaps mirroring the demographics of the survey, HIPAA (41%) and NIST 800-53 (21%) were strongly represented, important most directly to Healthcare and Government verticals. The ISO27001 Information Security Management System (ISMS) framework polled strongly at 28% reflecting its wide adoption worldwide across firms large and small. FedRAMP (12%) and PCI DSS (17%) also featured again mapping to industry verticals.

FIGURE 6: The percentage of organizations attempting to meet specific compliance frameworks and best practice standards



Interesting to note is the requirement to adhere to privacy laws. GDPR (17%), less than a year into its enforcement, impacts as many organizations as PCI DSS. More than half (52%) of those citing GDPR as a requirement were enterprise organizations, with most in the Technology, Manufacturing, and Financial Services sectors.

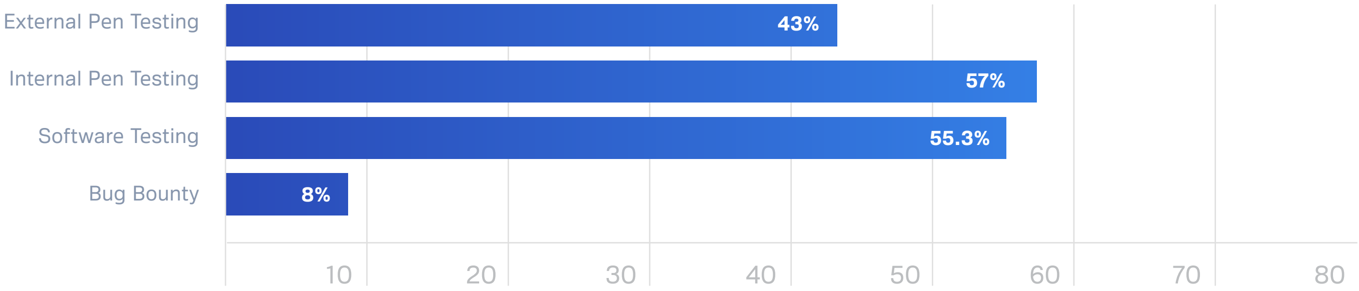
What methods do you employ to perform security testing for compliance purposes?

Security testing compliance standards generally describe requirements to mandate testing at both the application and network layer. Not only should data stores and applications processing sensitive data be tested, but also the underlying hosts and networks as well as other "connected" hosts and networks.

Our survey indicated that 55% of respondents were required to include applications and Software within scope of their program, but interestingly Internal Penetration Testing and Red Teaming (58%) led requirements for External Penetration Testing (43%). This could potentially be due to increasing regulatory-driven Red Teaming through schemes such as the Bank of England's CBEST scheme which have now been adopted by Financial Services (FS) regulators across the globe impacting systemically important FS firms.

Another testing method coming behind the four most common methods listed above is Crowdsourced Testing/Bug Bounty, which was used by around 8% of the organizations surveyed. According to Gartner, Crowdsourced Testing/Bug Bounty for compliance testing is a recent development (2018), and is expected to be used by 60% of organizations by 2022[1]. The majority of security testing for compliance today is still done using older methods.

FIGURE 7: The percentage of surveyed organizations who adopt specific testing methods



> *Crowdsourced Testing/Bug Bounty for compliance testing is a recent development (2018), and is expected to be used by 60% of organizations by 2022.*
>
> Gartner

[1] Gartner, *Market Guide for Crowdsourced Application Testing Services*

How many hours of testing are performed on average per test?

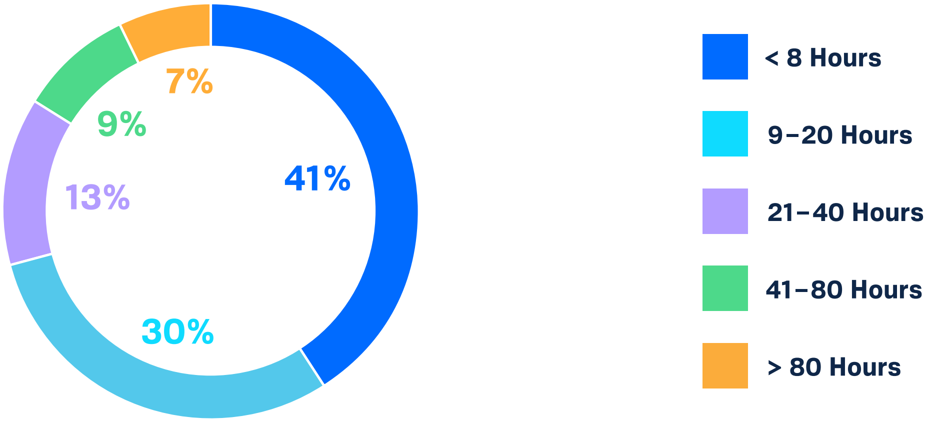
The time assigned to a security test can depend on the type of test, the number of systems involved, or the number of web pages and functions on a web site. A typical security test is one or two weeks long to provide sufficient time for analysis of security vulnerabilities.

However, our respondents indicated that on average a much lower number of hours were allocated. This could be due to budgetary concerns where teams have to cover many assets with limited budgets and team size or it could be due to finding it difficult to procure high quality vendor services.

The average organization allocates approximately 21 human testing hours per penetration test. Small to midsize businesses (SMBs) allocate the least amount of time to testing; nearly two-thirds of SMBs have less than 8 hours of testing per test.

New methods of security testing in the top 7% include Bug Bounty and Crowdsourced Security Testing. Both provide cash bounties to researchers, which provide extra incentives for additional hours on target when compared with a traditional time and materials security testing model. An average Crowdsourced Security Testing engagement has >300 hours of human testing per a penetration test according to data from recent engagements.

FIGURE 8: Percentage split of Average hours per Test

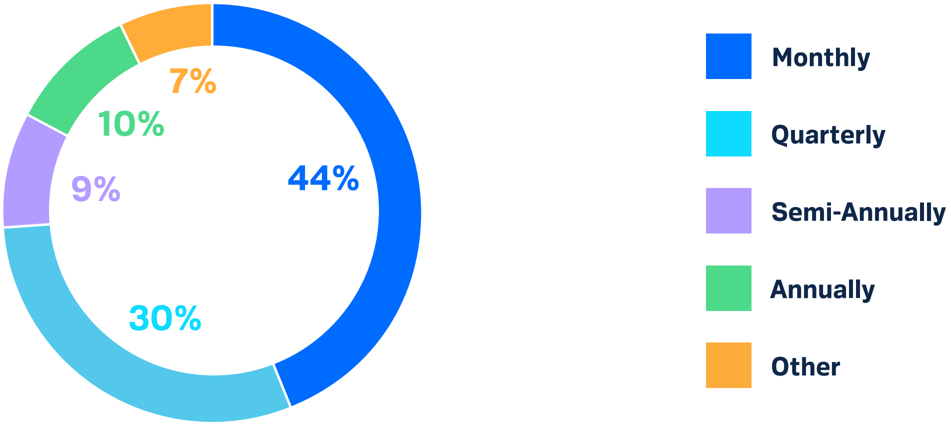


How often are you performing security testing?

More frequent product updates, a more dynamic attack surface, and an increase in the number and types of attacks require organizations to constantly monitor and verify their exposure. Continuous security testing is key for the assurance of an organization's security posture.

We asked organizations how often they were performing security testing to better understand their current level of concern and urgency when it came to assessing security risk (**Figure 8**).

FIGURE 9: How often organizations are testing security



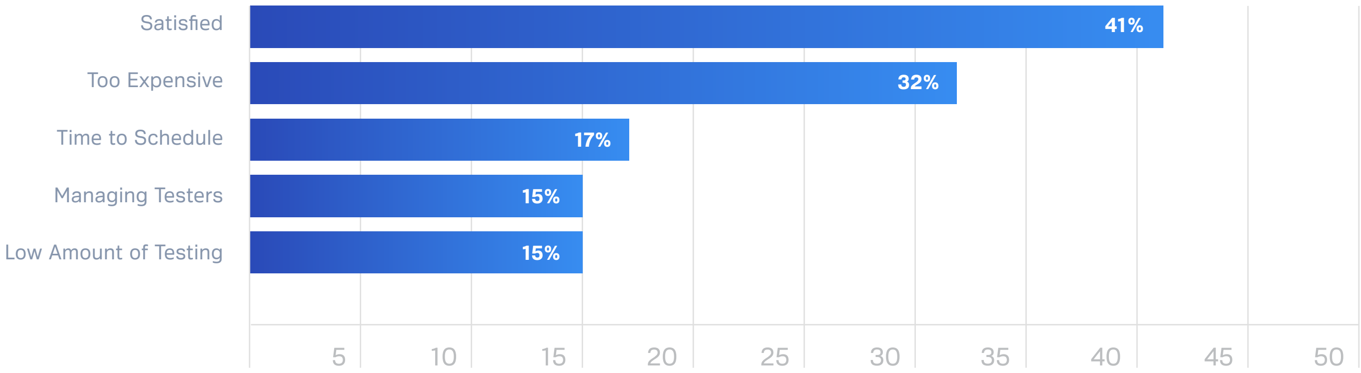
The responses were analyzed considering organization size, types of testing and hours spent per test and determined Enterprise organizations are more likely to have more complex testing requirements that are not solely based on regular testing intervals. Enterprise organizations' answers more frequently included continuously, scheduled, daily, weekly, and per release cycle.

It was also noted that organizations that utilize internal pen testing and crowdsourcing/bug bounties test more frequently than those that don't. As organizations perform testing more often, they also spend more time per test, indicating a resolute focus on maintaining high degrees of security.

What frustrates you about your current compliance testing process?

The process of security testing for compliance is complex and involved with many stakeholders across a highly specialist subject matter. Bridging teams across technology, security and vendor is challenging and driving successful project outcomes a challenge. When asked about frustrations of their current compliance testing process it is positive news that 41% of respondents were satisfied with their current process; however that does leave 59% dissatisfied. **Figure 9** highlights top frustrations.

FIGURE 10: What frustrates organizations about their current compliance testing process



The number one reported frustration was the process being too expensive (32%). Such cost concerns are not just related to test activity, but include the cost of remediation, the cost to scale efficiently, inefficiencies in integrating with DevOps processes and software pipelines and in dealing with false positives or low risk or poorly reported issues.

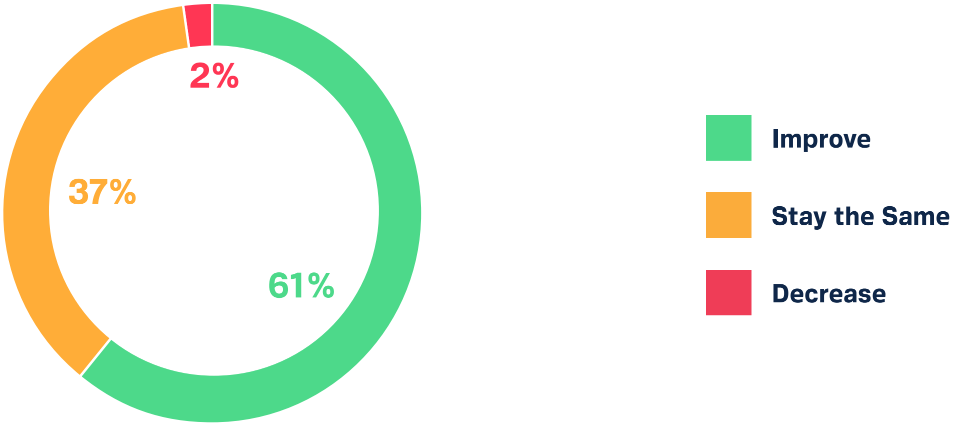
Traditional penetration testing approaches suffer, as reported, from issues around delays to scheduling tests impacting release cycles (17%), complex operational processes incurring overhead on technology teams and security teams alike (15%) and poor results from lower quality providers (15%).

> *“Such cost concerns are not just related to test activity, but include the cost of remediation, the cost to scale efficiently, inefficiencies in integrating with DevOps processes and software pipelines and in dealing with false positives or low risk or poorly reported issues.*

After a compliance test, how does confidence in your security posture change?

Security testing is used to identify and address found vulnerabilities as well as gain assurance in the security posture of a system or asset. We asked whether organizations felt more confident of their security posture post-testing. As shown in **Figure 10**, 61% of organizations feel they have greater confidence in their security posture and 37% report their confidence in their security posture is maintained.

FIGURE 11: How organizations confidence in their security posture changes after testing

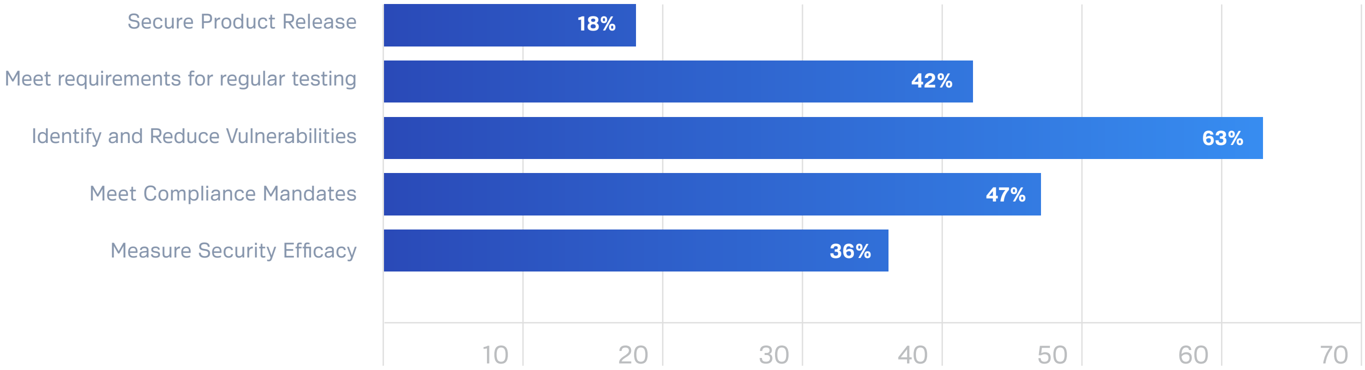


Vendor Strategy

In the last two years, how many vendors have assisted you with compliance and security testing?

Organizations use security vendors for a wide range of reasons including resource augmentation, to access specialist security skills that it is not practical to maintain internally or for an independent perspective, free from bias. The average organization is using more than two security vendors for their testing (**Figure 11**) while Enterprise organizations are using more than six security testing vendors. Not surprisingly, regulated industries, such as financial services, healthcare, and government, are using a higher number of security vendors.

FIGURE 12: Reasons organizations are using external vendors for compliance and security testing



Why are you using external vendors for compliance and security testing?

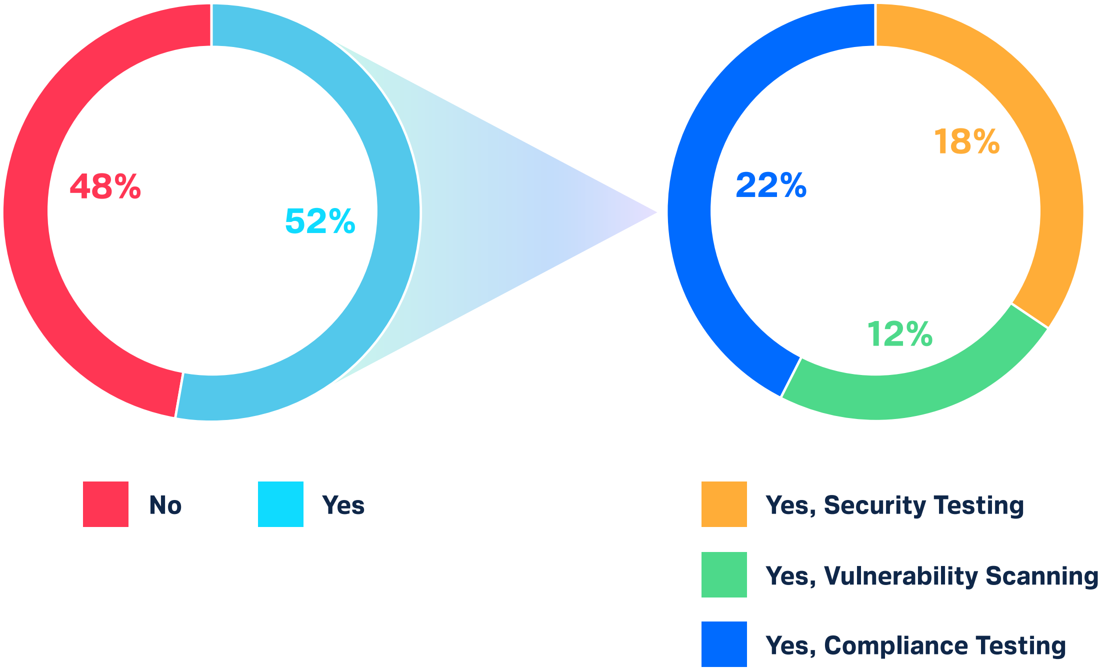
Where external vendors were used the most the most frequently cited reason provided was to Identify and Reduce Vulnerabilities followed by Meet Compliance Mandates and Regulation Requirements. It is positive to note respondent organizations are driving toward the importance of effective security and compliance.

> “ ***63% of organizations*** *use external vendors to identify and reduce vulnerabilities*

Do you believe there is overlap between your utilized vendor capabilities and if so, which category?

Utilizing multiple vendors increases complexity and administrative burden. If there is overlap in vendor capability this can creates unnecessary redundancy, inconsistent results and represent inefficient budget allocation. Enterprise organizations tend to source for best of breed vendors driving a higher number of vendors, whereas smaller firm trend towards use of single trusted partners. As shown in **Figure 12**, when asked about the perceived overlap, slightly more than half of organizations feel there's overlap of their vendors' capabilities.

FIGURE 13: Organizations who feel there's overlap of their vendors' capabilities and where they see overlap



Synack