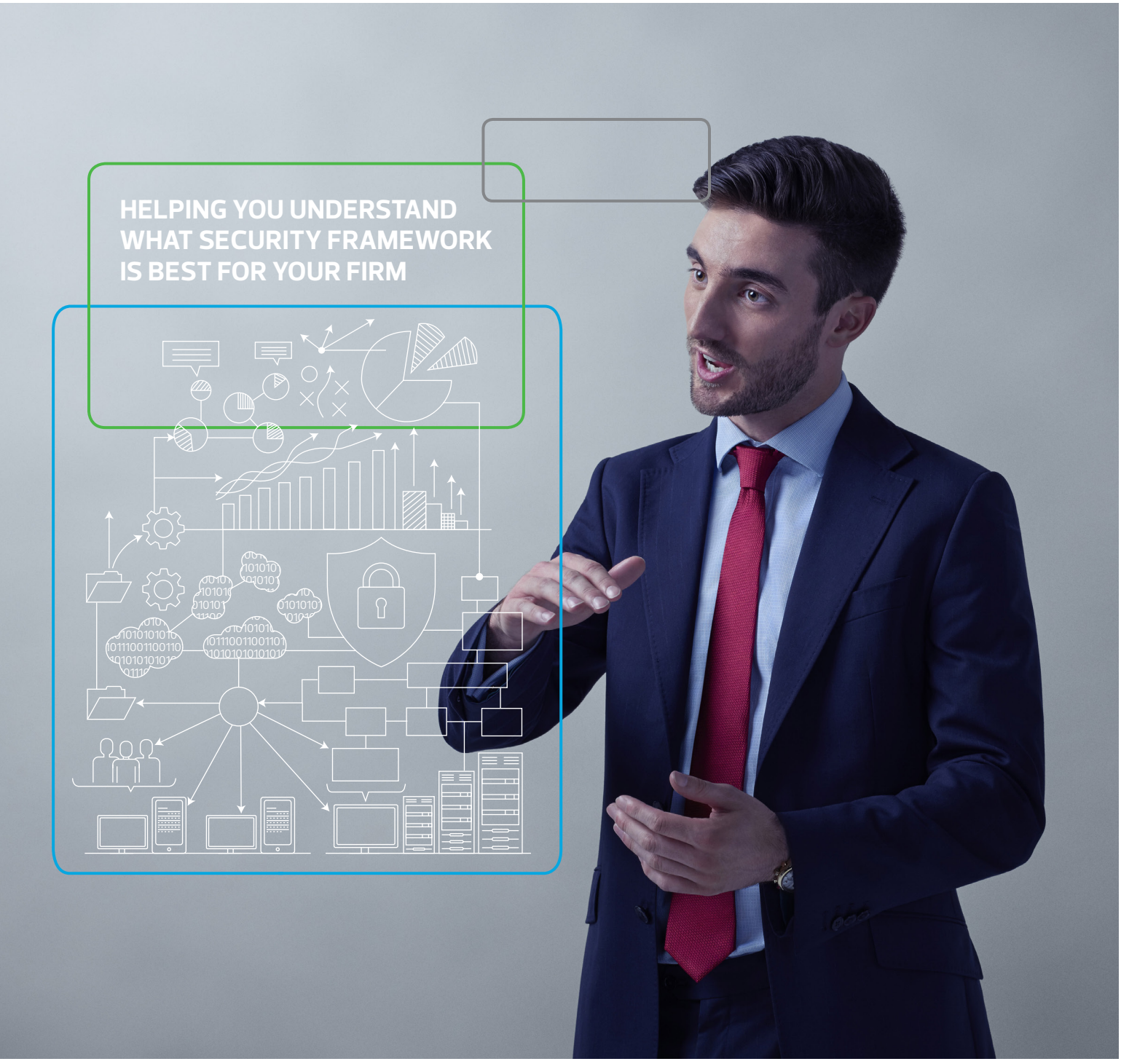



# SECURITY FRAMEWORK FOR LAW FIRMS

Research paper

# TABLE OF CONTENTS


**INTRODUCTION** 2

Industry uncertainty 2

The importance of selecting the right framework 3

**SURVEY FINDINGS** 4

Framework benefits 4

ISO 5

ISO advantages 5

Best for large, international firms 5

NIST CSF 6

NIST CSF gains in popularity 6

Best for established, growing firms 6

CIS 7

CIS yields results 7

Best for firms on a budget 7

PCI DSS 8

PCI DSS provides a flexible road map 8

A good fit for many 8

**NEXT STEPS** 9

Selecting a framework 9

Implementing a framework 10

Framework comparison at a glance 11

# INTRODUCTION

## Industry uncertainty

As massive data breaches and cyberattacks such as WannaCry and SamSam ransomware make headlines, many law firms are beginning to recognize the need for increased cybersecurity measures. Stolen or leaked data can directly affect clients, cause damage to a firm's reputation, and result in lawsuits, regulatory fines and loss of business.

Like most organizations, law firms are looking for guidance: What security framework is the best fit for our firm? How do we know if we've selected the right one? However, unlike other organizations, there is no single, clearly defined cybersecurity framework that applies to the entire industry. Instead, each firm is left to fend for themselves.

Individual law firms may follow the National Institute of Standards and Technology cybersecurity framework (NIST CSF), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the International Organization for Standardization (ISO) 27001/27002 standards for information security, or another framework such as the New York Department of Financial Services (NYDFS) regulations. That is a wide range of frameworks from which to choose.

To an extent, this diversity is necessary. A multinational firm with offices in 30 countries has different needs and abilities than a solo firm in small-town Wisconsin. Similarly, firms that specialize in health care law, criminal law or corporate law all function differently and hold different data. Personal injury or malpractice firms hold personal health information; criminal firms hold personal identifiable information; and corporate law firms hold financial and confidential data. As such, individual organizations may require different frameworks depending on their size, focus and goals. The key is knowing which one is right for you.

To select a framework, you must first understand why it was designed. Frameworks are like tools—each one has a purpose. You can use a screwdriver to pound in a nail, but a hammer is more effective. You can use a hammer to dig a hole, but a shovel works much better. Without an understanding of the advantages and disadvantages of each cybersecurity framework, firms cannot make an informed choice as to which framework to adopt.

That uncertainty has consequences for individual firms and the industry as a whole. Law firms face unique cybersecurity concerns due to the sensitive information they possess about their clients' legal or financial affairs. They are often easier targets for attackers because they may not have the same security budget or information technology (IT) staff as other industries due to the traditional focus on billable positions rather than operations personnel. Without the right framework in place, these organizations are at best inefficient, at worst left vulnerable. Moreover, if the firms that handle the legal affairs of almost every individual and organization in the country are at risk, the entire system is on shaky ground.

This research paper aims to correct the issue. RSM surveyed law firms across the country to determine what frameworks they are currently using and why. This data was then correlated with the self-reported effectiveness of each organization's security program and budgetary increases to determine which framework provides a best fit for different types of firms. By using this information to make the process of selecting a framework easier, law firms can begin to move forward with confidence and improve security for themselves, their clients and the world.

## The importance of selecting the right framework

Cybersecurity covers a broad range of practices: from data encryption to phishing awareness to patch management. With so many different aspects of security to consider and so many different frameworks to choose from, it can be difficult for organizations to implement any cybersecurity initiatives with confidence. As a result, law firms are less secure. For example, in 2016, RSM was able to compromise law firms and other professional service organizations during external penetration tests 60 percent of the time, the highest percentage of any industry.[1]

Selecting the right framework for your organization will cut through the confusion and provide clear, baseline expectations that are appropriate for your specific firm. Your team will no longer need to attempt ad hoc improvements because the right framework will provide specific direction that will help you make smarter security investments. In other words, instead of the doubt that comes with best guesses, your firm will have the assurance of best practices.

When Visa, MasterCard, Discover and American Express collaborated to establish the PCI framework and implement it throughout the retail industry, they were able to reduce millions of dollars lost to fraud each year.[2] If law firms can better identify and adopt the right cybersecurity framework, the potential impact to the industry could be just as powerful. That is why RSM conducted this survey to help your firm determine the best path forward.

### About the research

RSM conducted a survey of law firms between January and February 2018 to determine the effect of security framework mapping on cybersecurity budgets. Respondents represented a range of small, midsized and large firms (Figure 1). Nearly all respondents reported that their firm stored personally identifiable information (PII) (Figure 2), a majority (53 percent) store financial information and more than three-quarters (76 percent) indicate they store their data locally. Any substantial differences in responses among the type of respondents are noted throughout the report.

**FIGURE 1.** Survey participants by number of employees

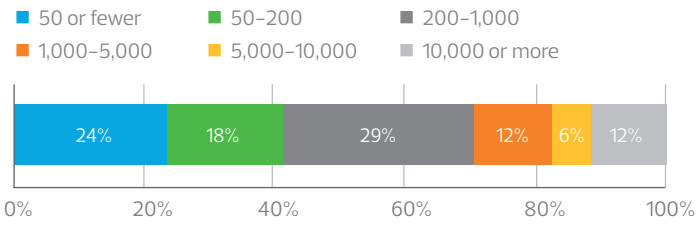
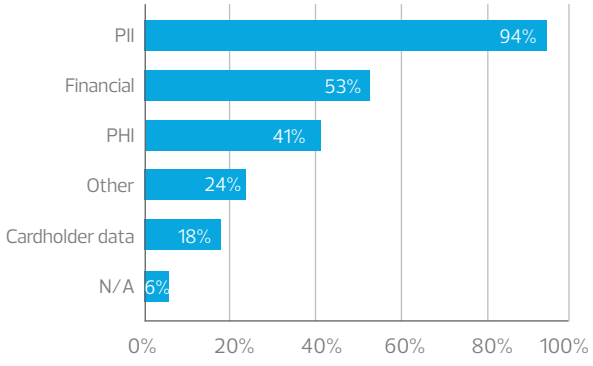



**FIGURE 2.** Type of data stored




1 "2017 Attack Vectors Report." SecureState.

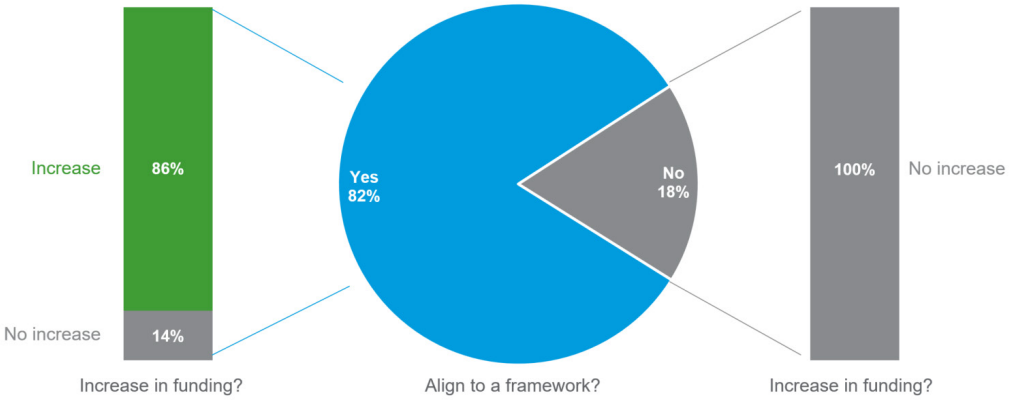
2 "Evidence for PCI's effectiveness in the fight against fraud." Federal Reserve Bank of Atlanta.

# SURVEY FINDINGS

## Our framework benefits

The central finding of our survey is that cybersecurity teams are significantly more likely to secure funding when aligning their security programs to a security framework. While firms that align to a framework may be funded differently depending on a variety of factors, those that do not align to a framework report that their cybersecurity budget has not increased at all over the past three years (Figure 3). In other words, without a framework, security teams have a difficult time getting the resources they need.

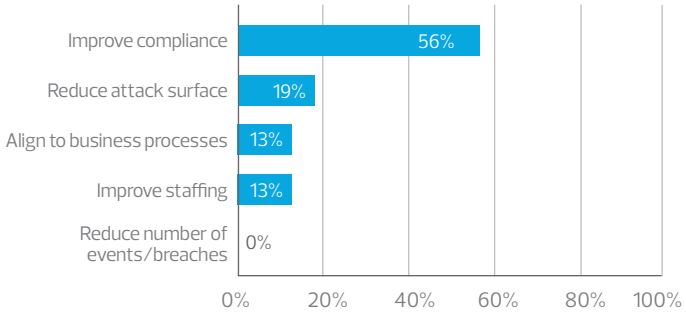
**FIGURE 3.** Impact of framework on cybersecurity budget




Aligning to a framework often correlates with budget increases because a majority of security teams use that framework to explain why they need additional funding. According to our survey, 56 percent of firms report that improved compliance to various existing frameworks is the biggest justification for an increase in the cybersecurity budget, beating out other reasons such as improved staffing and reducing breaches (Figure 4).

Organizations that hold data such as credit card information or protected health information (PHI) may be subject to the PCI or HIPAA regulations that drive some of the increased funding. Even so, aligning to any framework, regardless of legal or regulatory pressures, helps a security team support their case for a bigger budget. Firms can determine the quality of their security program by aligning it to a framework, and they can set goals based on the framework, as well as measure progress against it. By providing a way to quantify the rather abstract concepts of security and risk, frameworks give firms strong reasons for funding cybersecurity.

**FIGURE 4.** Biggest justification for budget increase



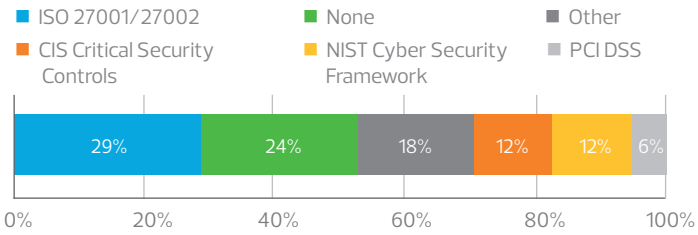

It's clear that aligning to any framework offers significant benefits. However, if firms select the right framework, it could make it even easier for security teams to improve their programs and obtain the funding they need. The question is: what are the advantages and disadvantages to each framework and which is the best fit for your firm?

## ISO

### ISO advantages

When we asked firms which security framework they followed, the largest percentage of respondents (29 percent) said they use ISO 27001/27002 standards for information security (Figure 5).

**FIGURE 5.** Frameworks followed




Because the ISO framework was developed with international standards in mind, it has a more global focus. ISO is aligned to the European Union's new General Data Protection Regulation (GDPR) standards that went into effect in 2018 and is the first-choice framework for firms that control or process data on EU citizens or organizations. ISO is also designed to apply to organizations of all sizes in all industries and all countries. As a result, it focuses less on technical controls than on high-level security processes and documentation.

In addition to being the top choice framework in our survey, respondents who map to the ISO framework reported some of the largest increases in funding for their security team. Every survey participant who aligns to the ISO framework said their cybersecurity budget increased on average, with two-fifths reporting an average funding increase between 11 and 20 percent. However, this may have been because international firms were spending extra money in order to comply with the GDPR standards before the May 2018 deadline.

### Best for large, international firms

While overall survey findings suggest that ISO is the best framework for the industry, a more granular analysis reveals that it may not be a good fit for every firm. Nearly 80 percent of survey respondents who map to ISO had over 1,000 employees, indicating that the framework is used primarily by large firms more likely to have international ties. Smaller or more regionally focused firms, however, may discover significant drawbacks to using ISO:

1. The lack of clear technical requirements in the ISO framework can be difficult for some firms, particularly those that cannot afford to employ a sizable and experienced security team.
2. Small or middle market firms may not do business overseas, and as a result, the GDPR-aligned framework with a global focus doesn't fit as well as the NIST CSF which was developed specifically for organizations in the United States.
3. The ISO framework is among the costliest frameworks to implement. Estimates for achieving ISO-27001 compliance vary in range depending on the size of the company, but it can easily reach six figures. This may prove too burdensome for many smaller or midsized firms. This may be why only about 1,500 organizations have actually gone through the expensive process to become ISO certified, even if they follow the framework internally.[3]

**ISO AT A GLANCE**

- Aligned with GDPR
- Focused on process and documentation
- Lack of technical detail
- Higher cost to implement
- Best fit for large or international firms

In other words, ISO is a strong choice for large, international firms that already have a relatively mature security program and are looking to comply with GDPR. Our survey revealed that the largest percentage of respondents map to ISO, and that they have seen an overall increase in cybersecurity funding. However, for firms simply looking for a clear, simple framework to get started, this expensive, high-level, international standard may not be the best fit.

3 "ISO Survey of Management System Standard Certifications" ISO.

## NIST CSF

Survey results indicate that there is no clear preferred framework for firms with fewer than 1,000 employees. Responses are split evenly between firms that map to the NIST CSF, the Center for Internet Security (CIS) framework or the Payment Card Industry Data Security Standard (PCI DSS) while nearly one in four firms does not follow a framework at all (Figure 5).

These findings underline the confusion in the industry and further demonstrate the need for clear information that can help firms select the best framework. RSM dug deeper into survey results to identify the strengths and weaknesses of these frameworks for middle market firms.

### NIST CSF AT A GLANCE

- Increasing in popularity
- Required for government agencies and some private partners
- More ambiguous and harder to implement
- Fewer resources available
- Best fit for established cybersecurity programs that work with federal organizations or government contractors

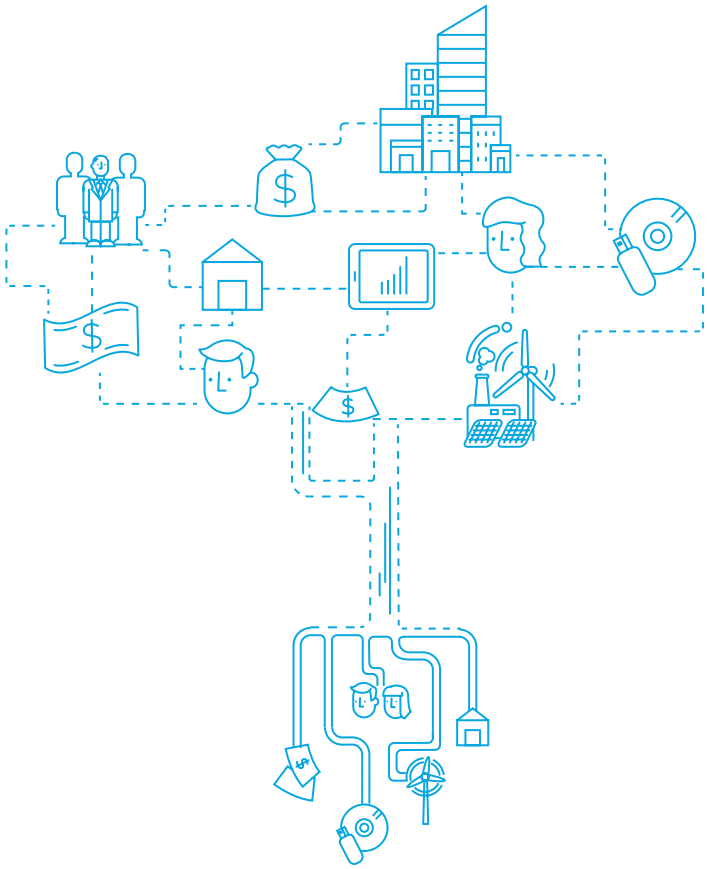
### NIST CSF gains in popularity

The NIST CSF, a framework developed by the U.S. government and first released in 2014, has increased in popularity in a short amount of time. Although originally intended for utilities and other operators of critical infrastructure, the framework is flexible enough to apply to a variety of industries. Government agencies as well as organizations or contractors that partner with the government often adopt the NIST CSF, and many private companies follow it as well, preferring the confidence and authority of a federally backed framework. This may be why some estimates project that 50 percent of U.S. organizations will use the NIST CSF by the year 2020.[4]

Although only 12 percent of survey participants reported that their security teams map to the NIST CSF (the second least of any framework included in the survey), these respondents indicated their teams received a funding increase of up to 20 percent on average over the last three years. This suggests that leveraging the reputation of the NIST CSF may be effective in convincing boards and partners to increase support for cybersecurity. If more organizations continue to adopt the framework, firms that follow the NIST CSF may find themselves not only well-protected but also well-positioned in the marketplace.

### Best for established, growing firms

Although the framework is growing in popularity, it can still be difficult to implement, particularly for firms without a security program currently in place. Compared to other frameworks, fewer resources are available to help build a program from scratch, and a 2016 survey of IT security professionals also indicated the framework requires a high level of investment.[5] Additionally, for firms just starting out, the flexibility of the NIST CSF approach may be too ambiguous and unclear. These smaller firms may be better suited following a simpler framework, preferably one that aligns with the NIST CSF, to leave open the possibility of an easy transition as both the organization and the framework matures. On the other end of the scale, large and international firms may find the nationally focused framework too limiting as it is not recognized outside the United States.



NIST CSF is the best fit for midsized or established firms that work with federal organizations, public utilities, government contractors or national companies dealing with supply chain management. It is also a strong choice for middle market firms looking to scale up nationally and position themselves for future growth. As a reliable framework with strong federal backing, the NIST CSF may be the framework of choice for forward-looking firms.

4 "Cyber Security Framework" National Institute of Standards and Technology.

5 "Trends in Security Framework Adoption" Dimension Research on behalf of Tenable Network Security.

## CIS

### CIS yields results

The CIS framework was developed by the nonprofit Center for Internet Security from which it takes its name. Developed by security experts, including the U.S. Department of Energy, law enforcement organizations and the National Security Agency (NSA), the framework focuses on the technical controls needed to maintain effective cyber defense by providing specific and actionable ways to stop common attacks. This practical focus is appealing. A homeowner may not need to have the latest, greatest and most expensive home security system to protect their house if a simple lock and alarm will do.

The CIS framework prioritizes a limited set of controls designed to yield the greatest return on investment. Perhaps this is why firms that map to CIS tend to provide more funding to their security teams. According to our survey, 18 percent of midsized firms map their security program to the CIS framework. These respondents also reported the largest increase in cybersecurity funding over a three-year period of any group.

### **CIS** AT A GLANCE

- Correlates with increased funding
- Strong technical focus
- Lack of guidance on process and program level
- Difficult to implement without support
- Best fit for firms with limited budgets

### Best for firms on a budget

Because CIS has such a strong technical focus, it is best suited for firms with strong technical personnel. Knowledgeable IT and security professionals can use their limited time and resources to focus on preventing and detecting the most common forms of attack. For smaller firms, in particular, this may be a better use of security funding than attempting to build the kind of comprehensive program that requires an entire team of full-time professionals.

However, many middle market firms may not have the resources to implement CIS without support. An effective cybersecurity program is more than just technical tools and solutions; it requires governance, oversight and ongoing program-level support. In other words, focusing on the most common attacks is an effective short-term strategy, but it can distract from long-term systemic security issues and leave the firm exposed. A small technical team will need guidance on secure processes and procedures as well as employee training and policy development, which the CIS framework does not offer. Supplementing an in-house technical team with high-level guidance from an outside security consultant, such as a virtual chief information security officer (CISO), can help smaller organizations begin building their own security programs.

While survey results indicated higher-than-average funding with CIS, we should also note these results may have been skewed by a statistical outlier—one participant who reported funding increases of over 50 percent. Although this framework may very well correlate with higher security budgets, the significant increase at a single organization could be attributed to other factors such as capital expenditures on upgraded equipment, which is only helpful when combined with an overall strategic plan.

Middle market firms with limited budgets may find that CIS provides the best bang for the buck, providing actionable defense for the most common attacks. However, even firms with limited budgets should recognize that technical controls are only effective with strong governance and management. In such cases, supplementing the IT team with management consulting resources specializing in cybersecurity could make the CIS framework a strong choice.

## PCI DSS

### PCI DSS provides a flexible road map

At first glance, the PCI DSS framework may not appear to be the best fit for law firms. Developed by the major U.S. credit card companies, the PCI DSS was designed to protect credit card information and is best suited for retail. Perhaps this is why only nine percent of survey respondents report mapping their security program to the framework. However, the PCI DSS fills many of the gaps left by the other frameworks, providing an established and comprehensive set of controls that are flexible enough to meet the variety of demands within the industry while remaining simple enough for small and middle market firms to implement without much difficulty.

**PCI DSS** AT A GLANCE

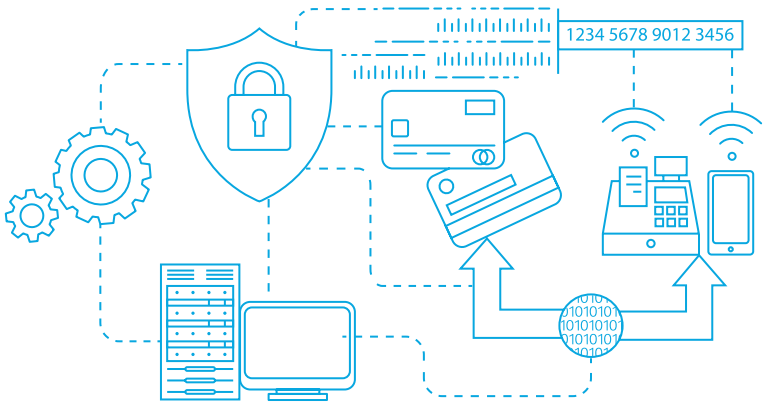
- Globally recognized, trusted, well-established
- Comprehensive and easy to implement
- Aligns with other frameworks (NIST CSF)
- Adaptable to different sensitive data sets besides cardholder data
- Best fit for most firms

First released in 2004, the PCI DSS has gone through three major updates and is a mature and trusted framework used by organizations around the world. Unlike the strictly high-level ISO framework or narrowly technical CIS framework, the PCI DSS provides comprehensive guidelines for an entire cybersecurity program. Firms can turn to the framework for clear requirements for everything from firewall configurations to patch management programs, infrastructure segmentation to security awareness training. PCI also uses a prioritized approach to building a security program, and there are significant resources available to help organizations of any size get started. The time and effort involved in getting a PCI DSS-mapped security program off the ground are much more manageable.

Although the framework was designed to protect credit card data, PCI DSS requirements are flexible enough that firms can substitute in any other sensitive data and still apply the same controls. While most firms may not need a cardholder data environment (CDE), all are holding sensitive data that needs to be protected in a secure environment. In this way, the PCI DSS framework can be applied throughout the entire organization. In addition, firms that handle financial information, sensitive legal documentation, PHI or any other confidential data can all apply the same framework without significant difficulty. The PCI DSS gives a diverse range of law firms a common set of regulations and best practices that can be adopted for sensitive data enterprise-wide.

### A good fit for many

One major drawback to following the PCI DSS is some organizations and industries do not accept the framework for compliance requirements or on security questionnaires. Certain clients or third-party partners may require your firm to align with a specific framework such as ISO, NIST CSF or CIS. While PCI DSS is flexible and can be applied to almost any type of sensitive information, a key client of yours not considering it as an acceptable substitute for a different framework could be a deal breaker. For this reason, firms should always review compliance requirements before committing to a framework (see the Next Steps section of this report for more information).




However, for firms that are not required to comply with a particular framework, PCI DSS provides a strong foundation for building and maturing a security program for all kinds of future development. Because it is prescriptive and comprehensive, organizations that map to PCI DSS are well-positioned to become compliant with other frameworks further down the road. If the NIST CSF continues to grow in popularity as predicted, for example, or if a new framework is developed, law firms that have mapped to PCI DSS will be ready to adapt as needed.

In such a diverse industry with firms of all types and sizes, the PCI DSS framework meets the needs of more organizations than any other framework. Although the PCI DSS was neither the most popular choice for law firms nor the framework that made the biggest impact on the security budget according to our survey, it is the strongest choice for middle market firms that don't clearly fit with another framework.

# NEXT STEPS

## Selecting a framework

Each framework is designed for a particular purpose and context. Identifying the framework that best fits your firm will help when justifying the costs of building and maintaining a security program. However, if your firm follows a framework that does not fit your needs, it can become a burden rather than an advantage. In the same way that using a hammer to dig a hole is ineffective, the wrong framework can drain internal resources, frustrate employees, lead to loss of contracts or clients, and even make your organization less secure.

For firms that already map to a specific framework, it is worth reviewing why that framework is being followed and determining whether there is a better alternative. For firms that are new to security, the following steps will help you select the right fit.

1. **Identify key data**
   Identify what regulated data you store (such as PHI or international data) to determine whether you must comply with a particular framework (such as HIPAA or ISO 27001). If you do not hold regulated data, then other confidential data or contractual obligations may steer you toward a particular framework. Overall, the data you have may dictate which framework is best for you.
2. **Assess client needs**
   Clients' interest in law firms' cybersecurity is growing rapidly. As more clients ask for questionnaires or detailed audits or reports from third-party testing, selecting the right framework can be just as much about the client as it is the firm. Firms working with financial clients or international organizations, for example, may prefer or require mapping to a particular framework. Targeting the framework of choice for your clients may be the key to not only a cybersecurity win but also financial success.
3. **Evaluate effectiveness**
   Following a framework is not just about checking boxes for regulators or clients; it is about protecting sensitive information. Consider the needs and resources of your firm to determine what framework can be implemented effectively. If your organization already maps to a framework, review whether implementation efforts have been successful. Aligning to business needs and operational effectiveness is key to a framework's success. Another option may be a better fit for your situation.
4. **Plan toward future goals**
   Selecting a framework should be a strategic choice that aligns with future goals. If your firm intends to target international clients, aligning to ISO now will position the organization for future success. Midsized firms based in the United States may align with NIST CSF to anticipate future growth. Working with executives and business leaders to identify business growth goals or changes will help you anticipate plans and select a framework with flexibility.

## Implementing a framework

The need for an effective cybersecurity program within the legal industry has never been stronger. With high-profile cybersecurity breaches making front-page headlines, more customers are looking for firms that make security a priority. For organizations that are new to cybersecurity, the challenges of building a program from the ground up can seem daunting. However, as law firms begin unifying around a common framework and working together to improve security overall, there's never been a better time to begin.

The following road map explains how to build a cybersecurity program that aligns to an established security framework:

1. **Establish a governing structure**
   To build an effective security program, you need an effective team. Select a program owner (e.g., a chief information security officer) to oversee the design, implementation and maintenance of the security program. Determine which individuals will act as data owners for critical data sets, and assemble a security steering committee with key members from security, operations and analysis teams to make strategic security decisions that advance the firm's mission.
2. **Perform a data discovery**
   A difficult but essential early step in this process is determining what type of data your organization stores and where it is located. Many firms do not have clear visibility into how sensitive data are brought into their systems, where it is stored or transferred to, who has access to it and how it is retained or destroyed. These are essential questions to answer in order to determine not only what technical controls need to be put in place to protect sensitive information, but also what process changes are necessary to streamline and secure data flow.
3. **Classify assets**
   Similar to data discovery, identifying and classifying assets—from servers to employee workstations to removable drives—is critical to building an effective security program. Once you know which assets are critical to the firm, you can prioritize how you apply security controls, conduct vulnerability remediation and prepare for incidents or disasters.
4. **Conduct risk assessment**
   Conducting a risk assessment will help provide a more in-depth review of the firm's risks and security posture, which are key in determining not only which framework to map to but also how it should be implemented. A risk assessment is a formal process of identifying, analyzing and documenting the security risks that may affect the firm. As such, the risk assessment lays the groundwork for developing a prioritized plan for moving an organization toward an acceptable level of risk, which is the goal of mapping to any framework.
5. **Apply controls**
   With a comprehensive view of your security program, you can then perform a gap analysis. Once you have identified the missing controls that must be applied to comply with your security framework, you can develop a remediation road map, implement changes and conduct independent testing to ensure the controls are in place.
6. **Develop security processes**
   As your security program matures, you will need to create consistent, repeatable processes to keep your network, systems and information secure. This involves developing configuration management programs for device hardening, patch management, vulnerability management and change management.
7. **Review program regularly**
   Finally, regular reviews and security assessments help identify not only new vulnerabilities but also opportunities to improve training, processes and technology. Continual improvement is the only way to protect your firm in an ever-shifting landscape, and this is exactly what security frameworks are designed to do—provide expert guidance and best practice recommendations for keeping your firm secure.

## Framework comparison at a glance

| | ISO | CIS | NIST CSF | PCI DSS |
|---|---|---|---|---|
| FOCUS | Designed for international consistency | Designed to prevent most common attacks | Designed for government agencies and some private partners | Designed to protect credit card data |
| BENEFITS | ▪ Aligned with GDPR<br>▪ Focused on process and documentation<br>▪ International acceptance for consistency around the world | ▪ Strong technical focus for practical protection<br>▪ Cost-effective approach for baseline defense<br>▪ Correlated with increased funding | ▪ Strong strategic focus<br>▪ Confidence and authority of government backing<br>▪ Positioned for future growth within the United States | ▪ Globally recognized, trusted, well-established<br>▪ Comprehensive and easy to implement<br>▪ Adaptable to different sensitive data sets |
| DRAWBACKS | ▪ Lack of technical detail<br>▪ Higher cost to implement<br>▪ Limitedapplicability for small, locally based firms | ▪ Lack of guidance on process and program level<br>▪ Difficult to implement without support<br>▪ Long-term strategic limitations | ▪ More ambiguous and harder to implement<br>▪ Fewer resources available<br>▪ Limited applicability internationally | ▪ Requires some customization<br>▪ May not satisfy industry-specific requirements |
| BEST FIT | Large or international firms | Technical firms on a budget | Growing or government-related firms | Most firms |

**+1 800 274 3978**
**rsmus.com**



tl-nt-ras-bp-0119-security frameworks for law firms report

RSM