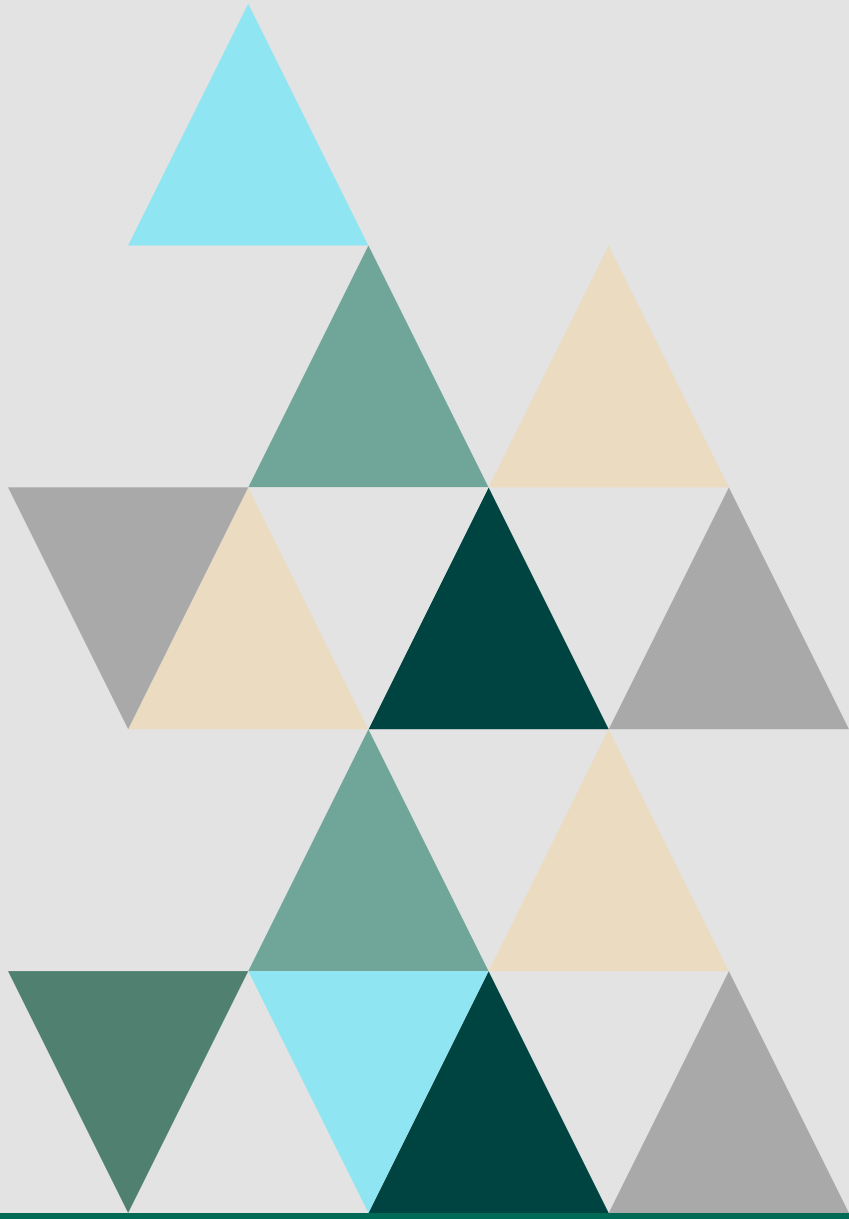
FORTRA™

Choosing the Right Cybersecurity Frameworks

What Experts Have to Say

Frameworks like the Center for Internet Security (CIS) Controls, MITRE ATT&CK, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework give organizations clear, step-by-step methodologies for protecting their sensitive data, leveraging a wealth of industry knowledge to take the guesswork out of your security program.

While these cybersecurity frameworks aren't mandatory like the Payment Card Industry Data Security Standard (PCI DSS) for organizations that process payments or the Healthcare Information Privacy and Portability Act (HIPAA) for healthcare organizations, using them in tandem with your required compliance policies is a tried-and-true way to harden your systems against cyberattacks.

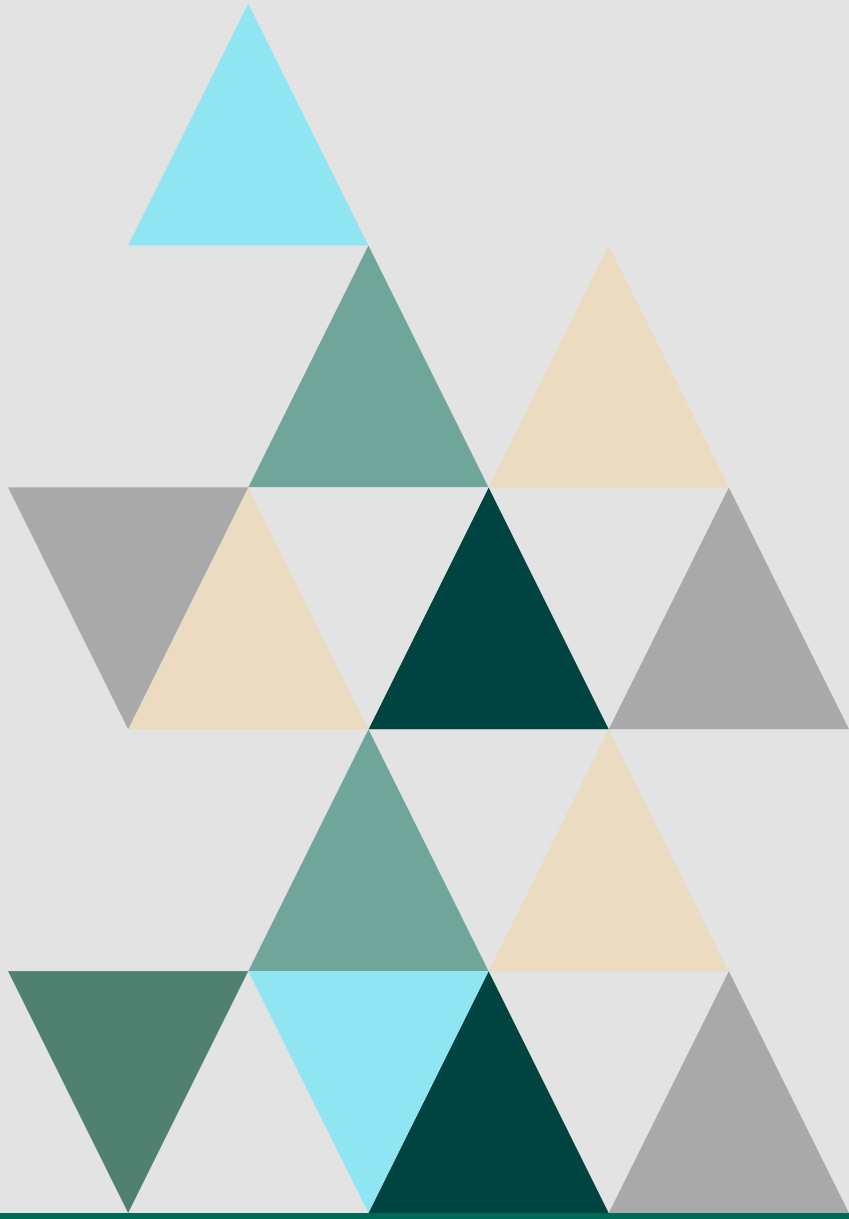


These types of best practice frameworks have been collaboratively built (and continuously updated) by experts for organizations like yours to use as a blueprint for your security program.

If you're ready to implement one of these frameworks, you might be wondering:

- *Is there one cybersecurity framework that gives the most payoff for the effort of implementation?*
- *What are some common mistakes people make when it comes to cybersecurity framework implementation?*
- *How should organizations go about picking the right framework for their circumstances?*
- *Is it advisable to apply multiple security frameworks at once? If so, what are the key considerations/steps needed to succeed?*

To answer these questions, Fortra surveyed nine top cybersecurity professionals to weigh in with their insights on the process of choosing the right cybersecurity frameworks.



Meet the Experts

Chris Hudson
Professional Services Architect, Tripwire

Tom Huntington
Executive VP of Technical Solutions, Fortra

Ambler Jackson
Cybersecurity Engineer, Noblis

Donnie MacColl
Senior Director of Technical Support, Fortra

Angus Macrae
Head of Cybersecurity, King's Service Centre

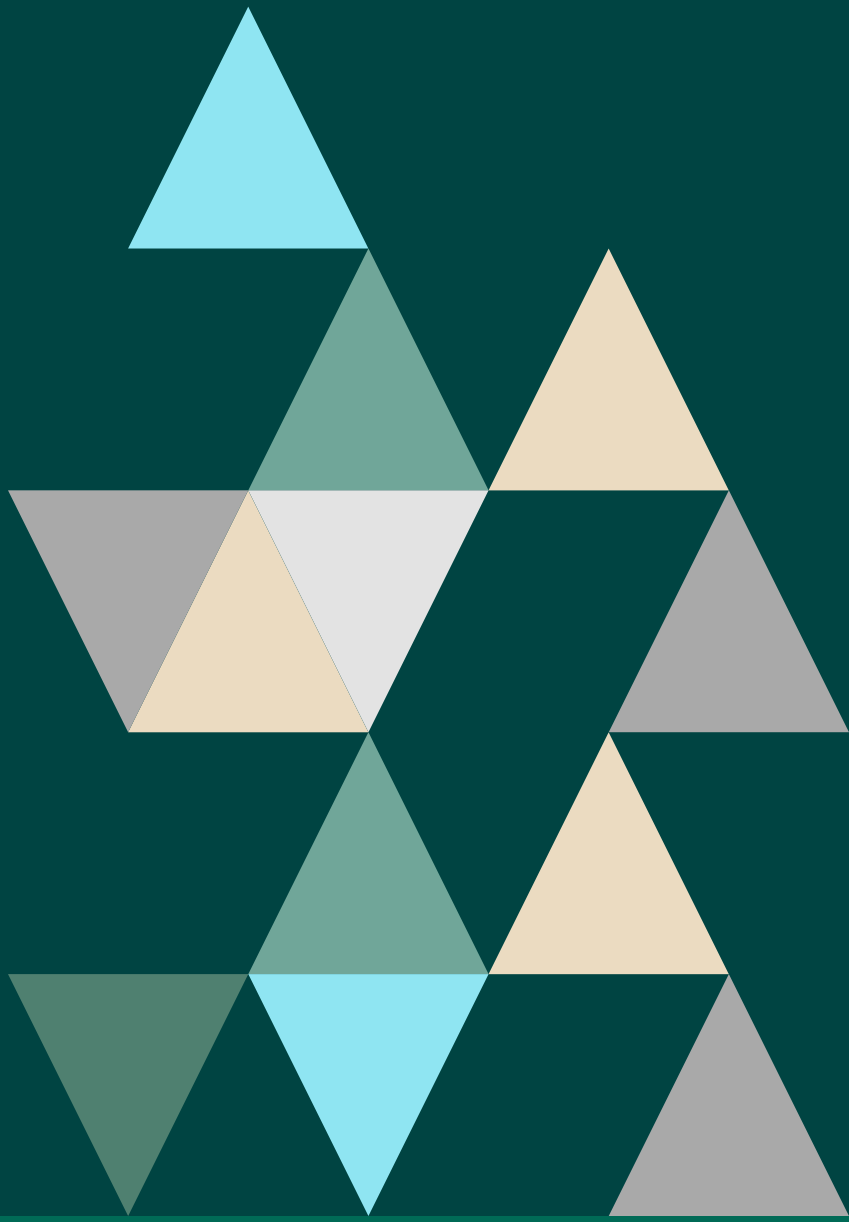
Zoë Rose
SecOps Manager, Canon EMEA

Antonio Sanchez
Principal Evangelist, Fortra

Amar Singh
CEO, Cyber Management Alliance Limited

Leron Zinatullin
Board and Startup Advisor and CISO, Linkly

Is there one cybersecurity framework that gives the most payoff for the effort of implementation?



Angus Macrae

Head of Cybersecurity, King's Service Centre

There is no one-size-fits-all framework that can answer this. All credible, industry-recognized frameworks will have their respective strengths, and their true value lies as much in how they are interpreted and meaningfully applied to an organization, as it does to the framework itself. The payoff for implementing a cybersecurity framework will always be very much influenced by the organization's specific needs, resources, mission goals, and objectives. It will also depend upon whatever the motivations for adopting it in the first place are and the areas you wish to measure improvement upon through its alignment.

For example, the CIS Controls may be a great practical start for someone looking more towards focusing on their technical IT controls and gauging defense-in-depth. Whereas an aspiration to align with the NIST Cybersecurity Framework (CSF) v2.0 at Tier 3 of "repeatable" or higher requires a far more holistic, organization-wide approach to managing cybersecurity risk at all levels, including at the most senior. The CSF does, however, offer a taxonomy of high-level cybersecurity outcomes based upon its core functional areas of Govern, Identify, Protect, Detect, Respond, and Recover, which will touch upon and thereby improve broader maturity across many areas of the organization, not just IT.

Antonio Sanchez

Principal Evangelist, Fortra

As always, the answer is, "It depends." It depends on whether the organization is bound by a specific mandate due to their industry, the customers they serve, the size of the organization, or some other requirement.

For startups and smaller organizations, I would suggest the CIS Controls. CIS Controls are practical, easy to follow, and have three implementation groups, which allows for tracking progress. If it's a larger organization where the perspective of business processes is needed, then I would suggest NIST Cybersecurity Framework. The NIST CSF was originally developed for critical infrastructure, but it ended up being widely adopted across all sectors. The current version (2.0) took this into account and made it easier to understand using common language and specific examples.

Chris Hudson

Professional Services Architect, Tripwire

The wide range of policies and detailed documentation offered by the Center for Internet Security (CIS) continues to be a popular choice in the field, and that makes a lot of sense to me. By covering more platforms, you can be sure of a more consistent approach to hardening. With up-to-date coverage for a wide range of popular devices, operating systems, and applications, I've seen far greater buy-in for implementation in the field, as there's less risk of conflicting advice between individual policy recommendations.

On top of this, I find the approach adopted with two levels of strictness (Level 1 and 2) in their policies to be beneficial since it allows you to target particularly critical areas of infrastructure with additional controls quickly and easily. This also encourages organizations to think about device criticality pragmatically which I think is another very useful step!

Finally, I've found implementing the individual CIS hardening controls to be easier for organizations with controls less likely to impact normal operational processes running on devices — many will leverage a few group policies to deliver high levels of compliance quickly and painlessly.

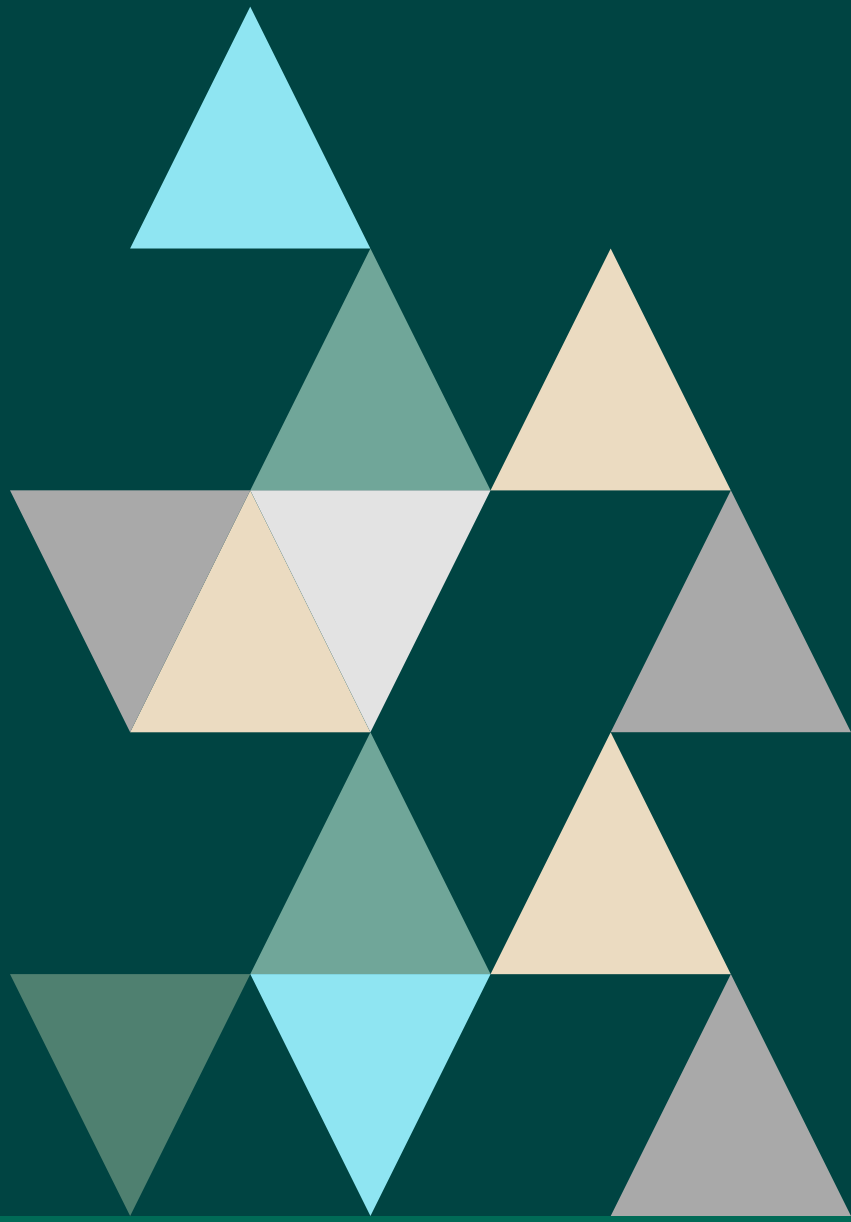
Amar Singh

CEO, Cyber Management Alliance Limited

This is a good question because everyone's looking for that one panacea of a framework. The simple answer, however, is no, because it depends on the context and risks and threats of an organization.

Reaching a bit deeper into the question, there are clear caveats for my reasoning. If you are accepting credit cards, then you obviously need to follow PCI DSS. And if you're a government, there are different frameworks in different countries. The spirit of the frameworks is important, because what any framework is trying to do is to reduce organizational risk.

What are some common mistakes people make when it comes to cybersecurity framework implementation?



Angus Macrae

Head of Cybersecurity, King's Service Centre

The belief that following any particular framework, standard, or certification achieves some elusive, endgame, 100 percent security nirvana is a dangerous myth. After all, our adversaries and threat actors have access to exactly the same frameworks and associated deployment guidance. But that's something any cyber professional already knows, of course.

It's also a message that the board needs to clearly understand from the outset, but one which may be hard for them to accept. Without strong support from board-level management, cybersecurity initiatives will invariably yield limited results. They may reasonably question why the cost, effort, and possible disruption of institutional adherence to any cybersecurity framework should be a priority if it indeed offers no solid guarantee of cyber safety.

It's, therefore, part of our job as security professionals to articulate why it doesn't mean that adoption of a framework is futile, quite the reverse. Correct and meaningful implementation of a credible framework still reduces risk and makes the adversaries' job harder while giving both customers and senior stakeholders confidence that the right things are being done in a measurable way, possibly opening the organization up to new opportunities.

Another critical mistake is an overemphasis on purely metrics-based compliance scoring from some myopic checkbox ticking and often perfunctory viewpoint. It can take time to both adapt a framework to an organization as well as adapting the organization to a framework in a meaningful way.

Chris Hudson

Professional Services Architect, Tripwire

The most common mistake I've found is not planning your approach to implementing the recommendations found by the assessment framework. Getting assessment data is great, but having a strategy, both short and long, that addresses the findings is key. For organizations that are just starting out, a "line in the sand" approach of making sure that scores never drop is a foundation that can be easily adopted and ensure consistency within the organization.

After that, it's all about breaking down the findings into workable fragments. Whether that's by platform (all servers or all Windows servers, for example) or by discipline (password policies, firewall hardening, unnecessary applications, etc.), working out where the stops you want to take along the journey is incredibly important.

I'd also say that there is not enough appreciation for achieving each part of your plan — there should be tracking to show just how far you've come so that when you're speaking to the rest of the business, you can sing the praises of the hardworking security and system owners who've helped make the journey possible.

Antonio Sanchez

Principal Evangelist, Fortra

Regardless of the framework, there are a few things security leaders should be mindful of when it comes to implementation:

Tailor the framework to your specific needs and ensure you have a way to measure effectiveness. This can be a combination of quantitative and qualitative data such as surveys, interviews, and dashboards.

Have a communication plan in place. There are several stakeholders, and you must ensure you speak on their level. This means multiple communications are needed to reach different audience types in the organization. At the very least, you have one for technical stakeholders where you can use jargon-speak and one for the business audience where you use business language and avoid technical jargon. The business audience will want to know how these initiatives align with the goals of the business.

Don't create a lot of friction. No one ever sets out to be the most secure organization in the world, so ensure you don't end up introducing a bunch of friction that gets in the way of productivity.

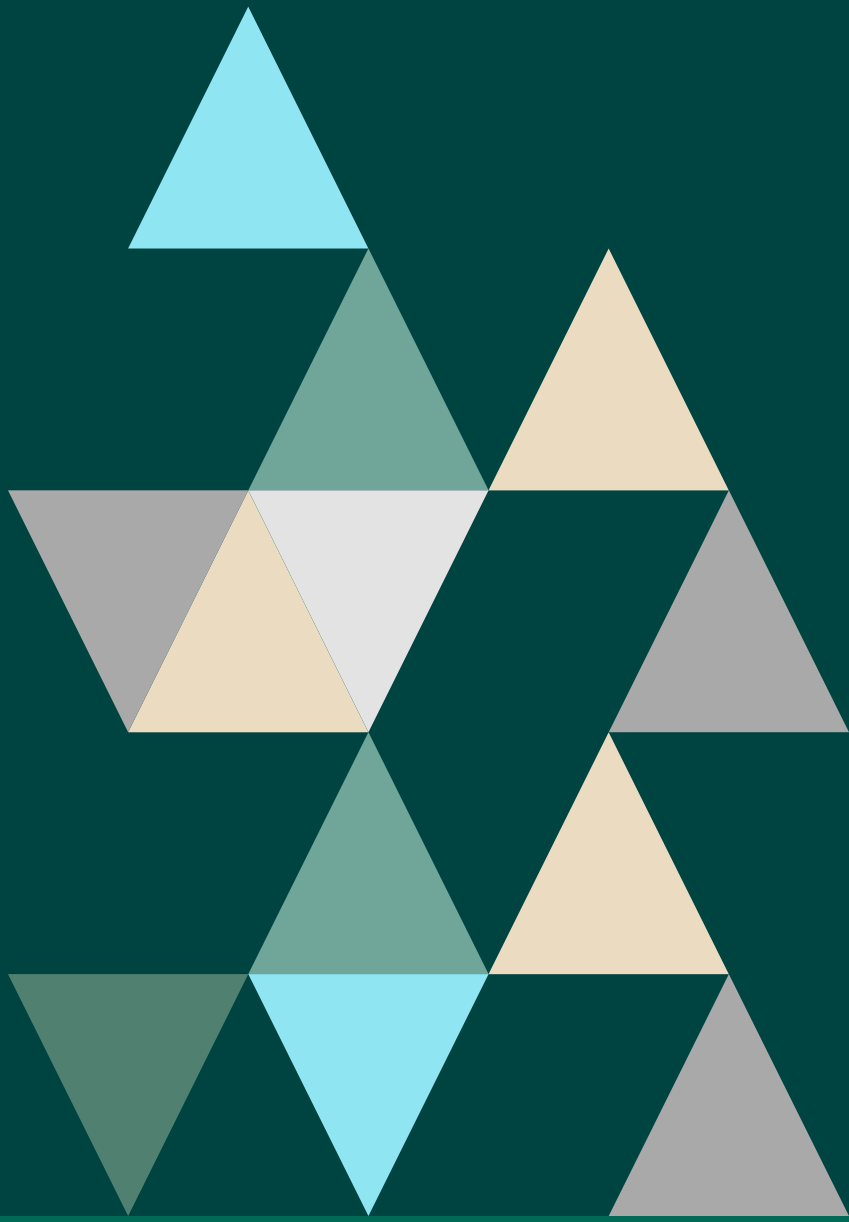
No shame culture. People make mistakes, and the sophistication of attacks can sometimes trick the most security-savvy person. Belittling and embarrassing users is unhealthy. A better approach is to build positive relationships with your users.

Amar Singh

CEO, Cyber Management Alliance Limited

Frameworks are very important, but sometimes, the problem is that people just look to satisfy the bare minimum rather than practice true security. The tick-box approach is problematic because we have clients coming to us about how to accomplish just that. We try to convince the customer that it's not just about ticking the box. By only accomplishing that, the spirit of the framework is lost.

How should organizations go about picking the right framework for their circumstances?



Tom Huntington

Executive VP of Technical Solutions, Fortra

When you think of frameworks for cybersecurity and the right framework, you must consider location, public trade, and industry. My first choice would be to look at what others are using in my industry, but I also consider the location (which country, state) where I am doing business. For instance, in Europe, I need to observe GDPR.

The framework you choose needs to span many regulations like PCI DSS, HIPAA, SOX, and more. We used to hear a lot about COBIT in the early era of SOX concerns, but in today's climate, NIST seems to be the most overarching framework. At the end of the day, the most important aspect is not just compliance and following a framework but also verification that my company's assets are secure.

Ambler Jackson

Cybersecurity Engineer, Noblis

Selecting a cybersecurity framework depends on many things, for example, the organization in which the industry operates, whether they have a mature cybersecurity program or if they have only recently begun their cybersecurity journey, and in some cases, whether they have the financial and human resources to implement the selected framework.

I do not think there is one cybersecurity framework that gives the most payoff for the effort of implementation because there are instances where an organization may need to make a business decision to use more than one framework, but if I had to recommend just one, I would recommend NIST CSF 2.0 due to its broad recognition and applicability (i.e., provides guidance to industry, government agencies, and other organizations). Also, organizations of any size can use the NIST CSF to reduce cyber risks.

Zoë Rose

SecOps Manager, Canon EMEA

There are many frameworks out there aimed at different use cases, but overall, they can often be mapped between each other. I think it's less of a concern to choose the perfect framework and more of an understanding of your goals. Frameworks are there to help move you forward, find gaps, and provide you guidance on the next steps — but they should never be used to justify a stop to continuous improvement.

A security roadmap should be aligned with the organization's risk appetite, understanding the competencies of the team, and the needs of the organization. When you understand this, you will be able to find a framework that looks to address these needs.

For example, many organizations make use of ISO 27001. This framework is a great way to start the discussion on formalizing workflows, documentation, and also signifying to external parties you have security as a part of the governance process.

The CIS Controls is a free framework that allows a bit more focus on technical controls and starts the discussion to ensure your policies align with what the business expects. Neither of these examples will ensure an organization is 100 percent secure because that's simply not possible. Choosing a framework is really about understanding your needs and aligning expectations.

Donnie MacColl

Senior Director of Technical Support, Fortra

Initially, you must research to understand your current baseline so you can measure progress and improvements. Talk with all departments and the executive teams to fully understand current and planned corporate strategy and external positioning and messaging, and from that outcome, determine and agree on the most suitable baseline framework as a starting point and other frameworks you plan to implement can complement and build upon.

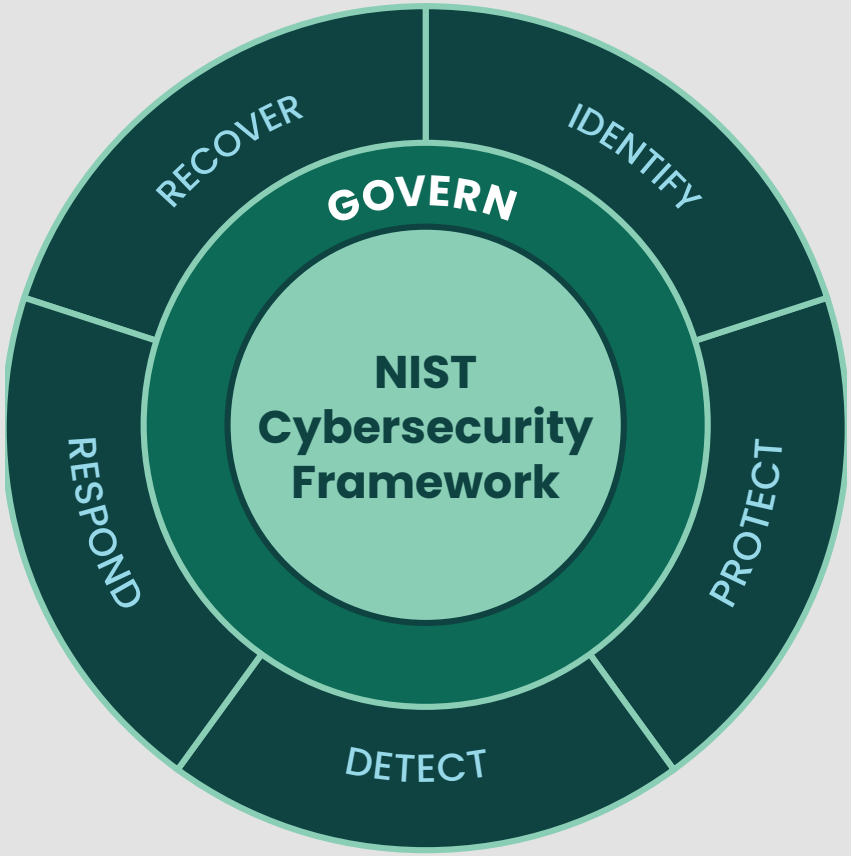
Pick one framework that encompasses the bulk of what you know you need to achieve now and implement that initially, knowing it is the first step on your security journey that sets you with strong foundations for other known and hopefully unknown frameworks that you will layer on top, with some overlap, in the future.

Leron Zinatullin

Board and Startup Advisor and CISO, Linkly

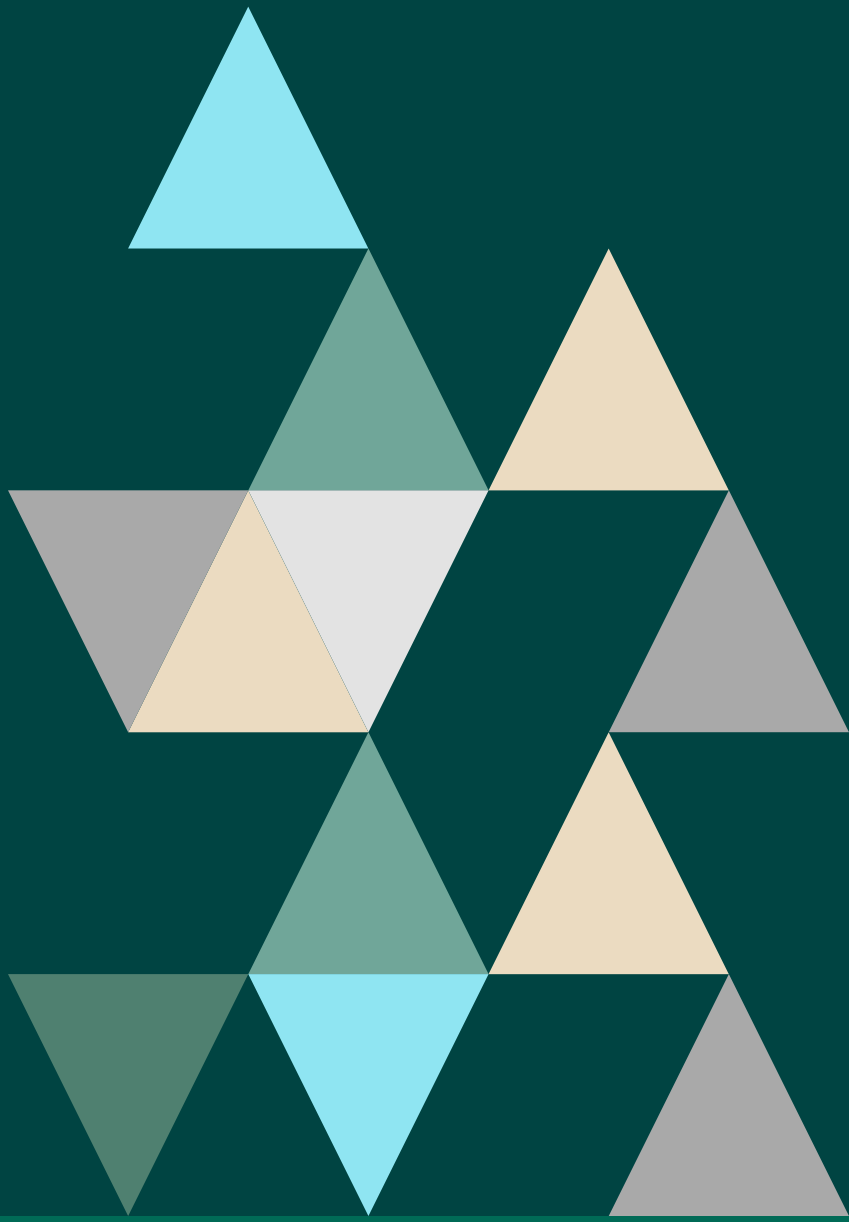
No single framework is a silver bullet — they all have pros and cons. Some frameworks are highly prescriptive and have a narrower scope — cardholder and account data for PCI DSS, for example. Some, like SOC 2, are more principled-based and don't mandate specific controls but rather Trust Services Criteria.

ISO 27001 is another popular choice. It's a risk-based framework, although it also has a set of example controls in the standard that many people choose to adopt. The NIST Cybersecurity Framework and its functions (Identify, Protect, Detect, Respond, Recover, and, more recently, Govern) can aid communication with business stakeholders, but it has its limitations, too. A particular industry may have other specialized sets of requirements, like NERC CIP for the electric power grid in North America.



Is it advisable to apply multiple security frameworks at once?

If so, what are the key considerations/steps needed to succeed?



Donnie MacColl

Senior Director of Technical Support, Fortra

At the risk of sounding controversial, I feel there are a few circumstances where applying multiple security frameworks at once does not make sense. As long as you have an initial baseline framework already implemented, then plan to implement the frameworks you are legally obliged to implement, and then those you feel meet the needs and goals of your company next after you have worked on a mapping exercise.

I suggest spending time upfront on a framework mapping exercise where you take your baseline framework and map across areas you already have covered with areas in the next two or three frameworks you wish to implement and check off areas that have already been implemented. All security frameworks will have common goals and common intent with their own added nuances, so you will quickly discover that you are already meeting some of the requirements of subsequent frameworks.

After mapping, pick the framework with the least additional requirements to implement, do it, and then add the next framework to your mapping exercise. The most important item to remember is to do something; small progress each day is better than no progress.

Ambler Jackson

Cybersecurity Engineer, Noblis

One common mistake security professionals make is moving forward with a linear process in mind. Organizations need to address multiple cybersecurity domains simultaneously to understand where gaps exist. Identifying gaps and weaknesses in cybersecurity domains will actually help practitioners select a framework that will ultimately guide their efforts to close the gaps and mature their cybersecurity program. Professionals can begin assessing all cybersecurity functions simultaneously. One does not have to attack one cybersecurity domain, reduce risk, and then move on to a second domain.

In fact, the NIST CSF 2.0 lays out six core functions that represent cybersecurity outcomes (Govern, Identify, Protect, Detect, Respond, and Recover), visualized in a wheel because they relate to one another, and the guidance in the CSF is to address the functions concurrently.

Leron Zinatullin

Board and Startup Advisor and CISO, Linkly

Many organizations are subject to multiple regulations and legislation simultaneously, having to adopt multiple frameworks and compliance regimes. If not managed appropriately, this can be labor-intensive to maintain and demonstrate compliance.

It helps to recognize that often, although worded differently, controls from different frameworks aim to achieve the same objective, so it pays to maintain cross-framework control mapping to streamline your compliance program.

While achieving compliance with a security framework is often a necessary step in establishing a baseline level of security, it's often not sufficient to mitigate modern threats. Compliance frameworks were developed with a specific objective in mind: to reduce risk. And they can get you part of the way there, just not all the way.

An organization can be compliant but still insecure. Security leaders should go beyond compliance and move towards actively identifying and managing risks, focusing on the overall security posture and risk reduction to survive and thrive in the digital world.

Zoë Rose

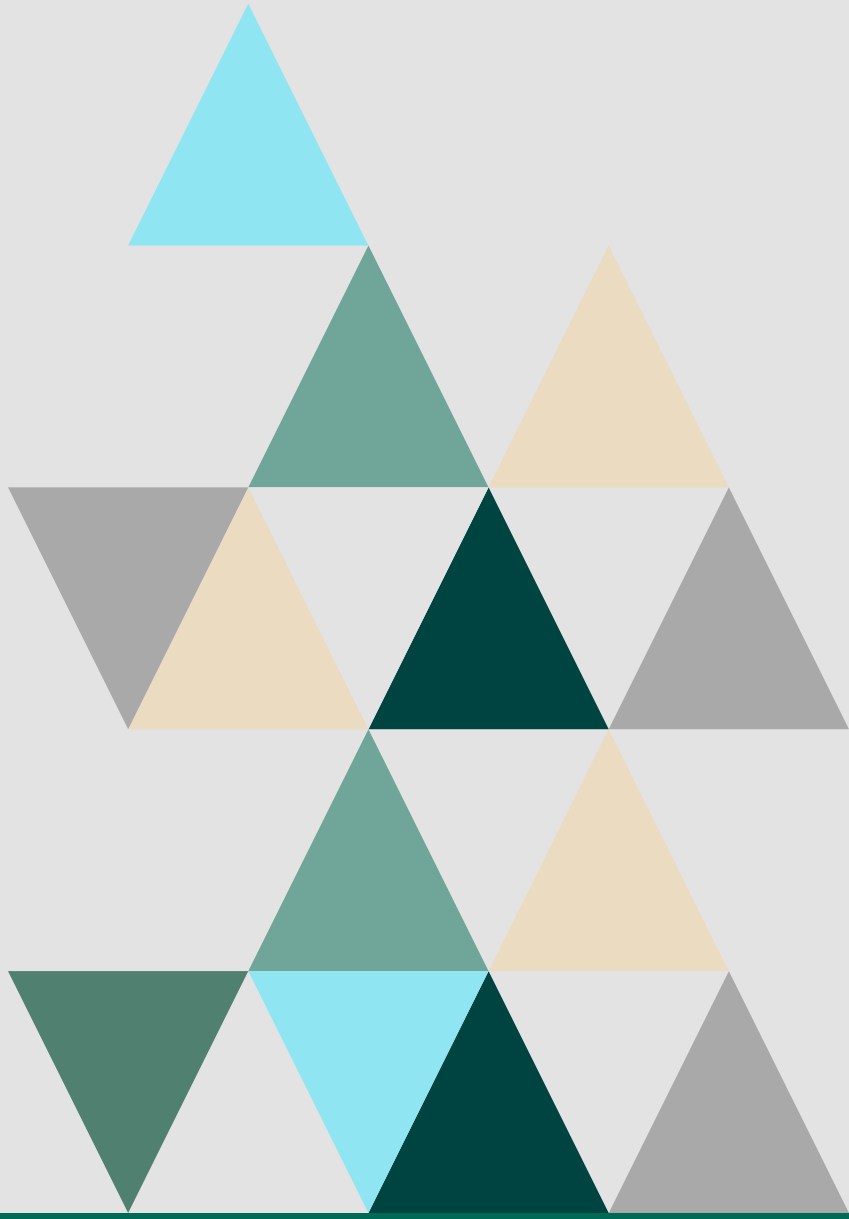
SecOps Manager, Canon EMEA

Having worked as a consultant for many years, I would say, from my experience, many organizations are not in a mature state where they can easily map their environment to multiple frameworks. I would suggest starting with one that makes sense for your environment and needs. Then, when you feel you have made some good progress, you can look at how another framework may enhance guiding your team to further organizational resilience.

What's Next?

When it comes to selecting the right compliance framework for your organization, Fortra's Tripwire is here to help point you in the right direction and answer any questions you may have. Tripwire offers solutions and services with built-in best practice policies like the CIS Controls, MITRE ATT&CK, NIST CSF, and more to help you stay one step ahead of cyber threats.

Learn how we can help you implement the right cybersecurity frameworks for your organization at fortra.com.



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-tw-gd-0524-r1-hm