VALLEY TECHLOGIC

2022

CYBER SECURITY FRAMEWORK OVERVIEW

By Rory Reed

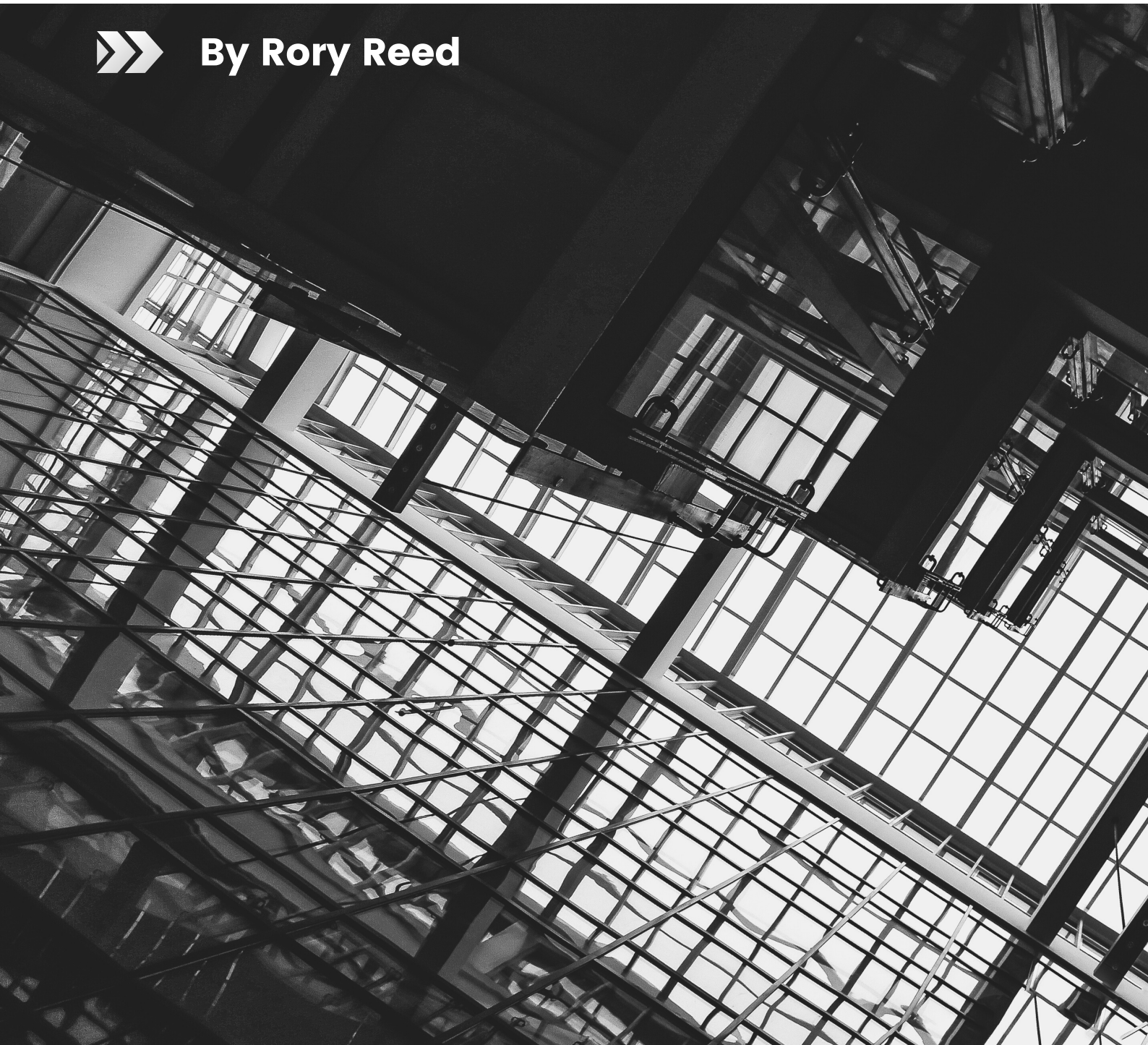


TABLE OF CONTENTS

WHAT IS A CYBERSECURITY FRAMEWORK?

Cybersecurity frameworks are designed to bring order to chaos. Many businesses bring new technology into their business on an as needed basis, this means older technology and newer technology are often co-mingled and cybersecurity measures are put on the back burner as new technology roll outs prioritize company resources.

Utilizing a cybersecurity framework gives your business highly attainable cybersecurity goals, every framework our business recommends includes goals that slowly scale in difficulty, starting with basic measures such as better password hygiene and enabling two-factor authentication all the way up to more complex measures such as advanced documentation of internal and external data streams within your business and creating metrics from the cybersecurity software your business invests in (or that's supplied to you by your IT provider).

Once your company commits to a cybersecurity framework you will find that it's easier to go forward with new technology choices with renewed confidence. It's more difficult to fix problems that already exist but once you do, managing and maintaining those efforts is easier and highly worthwhile.

In this information packet, we will explain the three types of cybersecurity frameworks that exist, the three frameworks on the market we personally recommend for businesses as well as an overview of HIPAA for the medical sector, and how we can help you with implementation.

A MESSAGE TO BUSINESS OWNERS

Choosing a cybersecurity framework that's right for your business depends on a number of different factors.

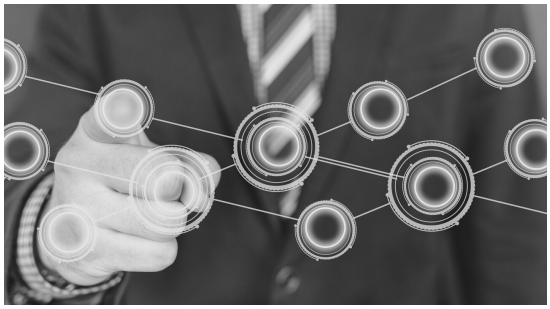
Not every businesses cybersecurity needs are the same. Businesses with a more consumer forward presence and/or those that regularly handle Personally Identifiable Information (PII) will have a higher cybersecurity need than a company that only has other businesses as clients and/or one with a very low technology footprint.

We also discuss the framework currently being required by the Department of Defense (DoD) for defense contractors and subcontractors. Any framework you choose will help protect your business, but choosing the right one will make for a much smoother roll out with an appropriate level of cyberthreat protection.

Read on to learn more about the NIST, CMMC, HIPAA and CIS Cybersecurity Frameworks.

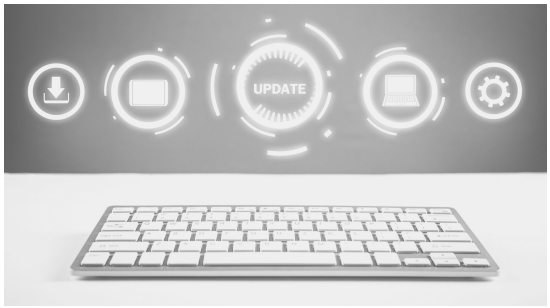
TYPES OF FRAMEWORKS

While we're only going to cover what we feel are the three main cybersecurity frameworks out there, cybersecurity frameworks fall into these three categories.



Control Frameworks:

- Develop a basic strategy for security team
- Provide baseline set of controls
- Assess current technical state
- Prioritize control implementation



Program Frameworks:

- Assess state of security program
- Build comprehensive security program
- Measure program security/ competitive analysis
- Simplify communication between security team and business leaders

Risk Frameworks:

- Define key process steps to assess/manage risk
- Structure program for risk management
- Identify, measure, and quantify risk
- Prioritize security activities

You should pick a cybersecurity framework that most aligns with your business's goals for cybersecurity and technology. Choosing the right framework type will allow you to quickly bring your business up to speed and meet compliance goals according to local government regulations, services like cybersecurity insurance, or goals set by your clients.
Valley Techlogic can assist you in choosing the right framework for your business.

NIST FRAMEWORK

The NIST Framework for Improving Critical Infrastructure Cybersecurity usually shortened to just the "NIST Cybersecurity Framework" is one of the more well known cybersecurity frameworks and it's broad in both it's scope and complexity. As with all of the frameworks we're mentioning in this document, the difficulty of the steps scales as you move up through the tiers. The basic components found in the first tier of the NIST Framework are an excellent place for businesses of any size to start.

We recommend this framework to clients looking for a stricter path to follow to protect their organization from cyberthreats. To start, we will create a "Current Profile" for your organization following an assessment performed by us, as well as a "Target Profile". Our assessment will address your current concerns as they relate to cybersecurity and the "target profile" will represent goals you hope to accomplish across a timeline we will help establish.

The NIST Framework features five separate tenets (shown in the graphic below) and five tiers. Within those five tiers there are over one thousand components known as controls. Only the most strict cybersecurity environment will need to work towards implementing all of the controls, for most businesses working towards tier three will be more than sufficient and attainable. Our assessment will give you a guideline for which tier is most appropriate for your business.

CMMC FRAMEWORK 1.0

The Cybersecurity Maturity Model Certification (CMMC) Framework was created by the Department of Defense (DoD) to help defense contractors and subcontractors protect the sensitive Controlled Unclassified Information (CUI) they receive as part of the defense contracts their business is awarded by the government. This framework is heavily influenced by the NIST framework and also scales in difficulty. For most contractors, to be compliant with the contracts they receive or bid on they will need to work towards obtaining at least maturity level 3. They will also need an outside CMMC security or technology consultant to validate and certify their efforts.

Maturity	Number of Controls	Goal
Level 1	17 Controls	**Practices: Basic Cyber Hygiene:** Level 1 focuses on the basic elements of cyber hygiene, such as better password implementation
Level 2	72 Controls	**Practices: Intermediate Cyber Hygiene:** Level 2 scales the difficulty up, increasing documentation practices and preparing for the elements of level 3
Level 3	130 Controls	**Practices: Good Cyber Hygiene:** Level 3 puts practices in place to mitigate cyberthreats as well as a response plan if a cyberattack were to occur
Level 4	156 Controls	**Practices: Proactive** Level 4 further builds on the foundations put in place by levels 1 through 3, more effectively mitigating cyberthreats as well as developing evolving strategies to combat them
Level 5	171 Controls	**Practices: Advanced/Proactive** Level 5 involves putting the most sophisticated cyberthreat tool available s in place in your business to protect CUI data.

CMMC FRAMEWORK 2.0

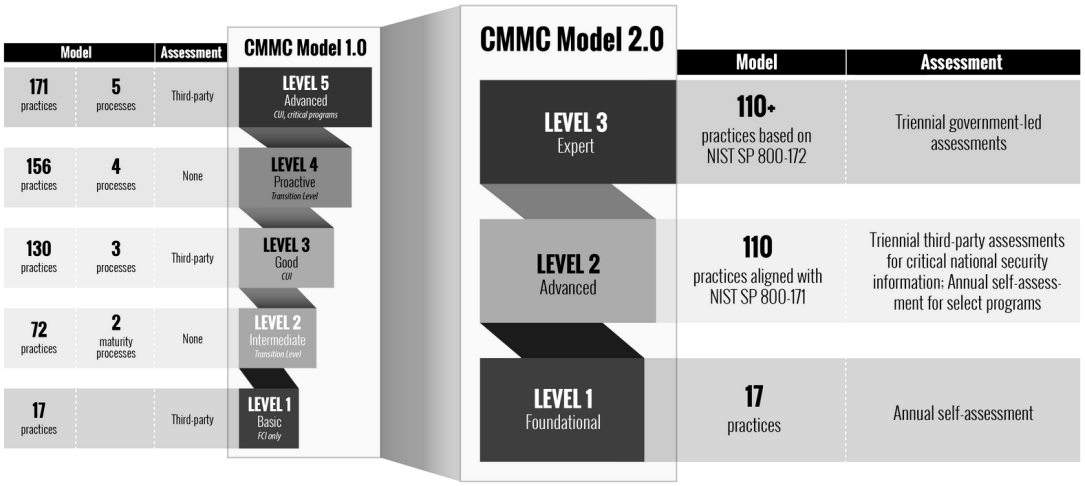
On November 4th, 2021, it was announced that a version 2.0 of the Cybersecurity Maturity Model Certification (CMMC) Framework was in the works and being suggested as a more attainable model of certification for defense contractors and subcontractors. This model will more closely follow the NIST Framework, removing all of the CMMC specific controls and streamlining the process to just 3 maturity levels.

This version of CMMC will not be in effect until a ruling is had, which could take anywhere from 9 to 24 months. We're advising our clients to continue to work towards obtaining maturity level 3 in the existing model so that if and when version 2.0 is implemented, they will be in an excellent position to certify for level 2 or 3 of that version.

Also implemented in 2.0 will be the ability to self certify for maturity level 1, these self certifications will need to be conducted annually. If your business currently contracts with the DoD but does not handle CUI that may be all that is required of you, if your business does handle CUI it's our recommendation that your organization continue to work towards obtaining maturity level 2 or 3 in the existing model.

In version 2.0, organizations that obtain maturity level 2 will need to be certified by third party technology consultant, and for maturity level 3 your business will need to be certified by a government-led assessment. These assessments will occur triennially for those maturity levels.

Valley Techlogic is able to bring businesses to compliance up to maturity level 3 in the existing model, we have tools and software that meet the compliance requirements and can assist your organization with your certification goals.



CIS FRAMEWORK

The Center for Internet Security (CIS) Framework was built in the late 2000's by unpaid volunteers who were experts in the cybersecurity field, it was their hope to lead a grassroots effort to bring a layer of cybersecurity safety to workplaces and unite the global workforce to help put a stop to cyber crime. It is comprised of 18 controls that stem from various fields, such as government, education, healthcare and more.

This makes this framework a good fit not just with B2B organizations, but that means it also meets the criteria for HIPAA and other industry specific compliance standards. The controls found in CIS are highly implementable for businesses of all sizes, the framework provides a detailed blueprint to keep your business safe from cyberthreats.

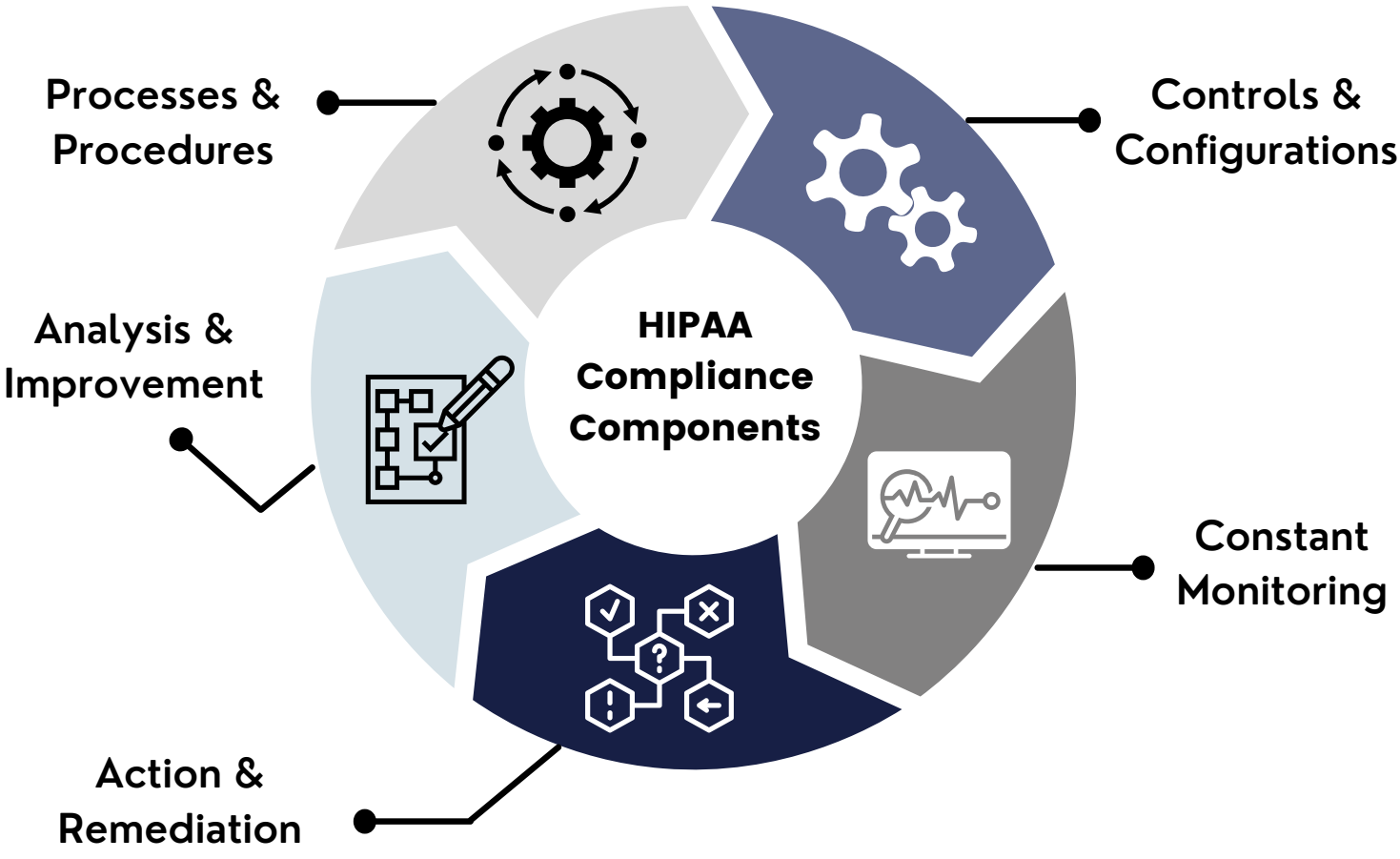
As with NIST and CMMC, CIS takes a tiered approach which allows you to bring your business to compliance at your own place through the step by step process, and Valley Techlogic is equipped help your business implements those steps. Below are the 18 controls found in V 8.0 of the CIS Framework.

HIPAA FRAMEWORK

HIPAA shares many of the same components of the other frameworks we have mentioned, although it predates many of them. Released in 1996, the Health Insurance Portability and Accountability Act (HIPAA) was created to bring a unifying set of standards to the healthcare industry in order to protect Protected Health Information (PHI).

NIST even published a guide to HIPAA in 2008 called "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP 800-66 Revision 1)" because there are so many shared standards between the two of them. As with all of the other frameworks, maintaining your compliance is not a one and done activity. It's an evolving process that changes with the threat landscape.

Valley Techlogic has assisted our medical sector clients in obtaining greater compliance with HIPAA standards. You can see the steps we use below to accomplish that goal.



HOW VALLEY TECHLOGIC CAN HELP YOUR BUSINESS

Valley Techlogic has tools in place to help businesses of any size located in the Central Valley implement the best cybersecurity framework choice for their business and to help bring them to compliance and meet their cybersecurity and technology goals

- We have invested in compliance software that meets the criteria for NIST, CMMC, CIS and more
- Our employees are trained on the best cybersecurity practices
- We believe in proper documentation and reporting,, another critical compliance factor
- We regularly check in with our clients via quarterly or annual Technology Business Reviews (TBR)
- Our plans offer a best in class technology experience for clients, it's like investing in a full scale IT department for your business without any of the overhead necessary to maintain it, we handle your IT so you can handle your business

Thank you for taking the time to read this packet, for more assistance in choosing a cybersecurity framework or about our other technology services, reach out to us directly via the contact information below.

Contact

VALLEY TECHLOGIC, INC

111 Business Park Way, Atwater CA 95301

209-357-3121

www.valleytechlogic.com

sales@valleytechlogic.com

@Valley Techlogic