July 13, 2022

**Easy-Button CMMC**



Easy-Button CMMC

By this point, if you are a Federal Supplier that is impacted by the mandates, you are well aware.  We do not need to explain the mandates to you.  Do you need help planning, deploying, and running your cloud environments & collaboration platforms to ensure compliance with Federal Regulations before the deadline? If so, we can help!

Why is CloudFit Software discussing this topic?

CloudFit Software brings unique perspective on this topic for many reasons including the following:

1. CloudFit Software is a DoD company that also *intentionally* serves large and small commercial, government and DoD entities across all sectors from **Healthcare** to **Finance** to **Manufacturing** to **Cloud Provider** to **Independent Software Vendors (ISVs)**to **State and Local Government** to **Law Enforcement**to **DoD** to **Defense Industrial Base**. It is intentional. Commercial work keeps us on the cutting edge, and that is attractive to DoD.  If we can provide Managed AppDev, Managed Data/AI, Managed Cyber and Managed Services to Microsoft’s own Product Groups, we can do it successfully for anyone.  DoD work means that we know true Cyber, and that is attractive to commercial customers.  Therefore, we are uniquely positioned to guide those beholden to the CMMC mandates.
2. CloudFit has won Microsoft’s US Partner Award for Government / Defense and Intelligence the past two years in a row. We know what we are doing, and we execute well.  Customers and Microsoft attest to it.  We earn and maintain trust.
3. CloudFit has a patented platform that is fully accredited that allows us to move faster and cheaper than everyone else with greater quality. Our Intellectual Property is within the toolset and goes with us to every customer thereby allowing every customer to benefit from our learnings at every previous customer.
4. CloudFit is doing it at scale across our customer base. Our smallest managed customer has 5 users.  Our largest has well over 1M users.  We are scale.
5. These managed-easy-button-solutions-and-outcomes are CloudFit’s core business. [CloudFit? Just say YAaaS! – CloudFit™ (cloudfitsoftware.com)](https://www.cloudfitsoftware.com/cloudfit-just-say-yaaas/)

Now that you understand a handful of the reasons why CloudFit should have a voice on this topic, let’s move on to execution.

The open question is likely “how do I become compliant”?   Ultimately, there are two options.  But before we get to the options of how to become compliant, we first need to address the scope of what needs to become compliant.

What about scope?

There are thousands of other published pages on the scope of CMMC, and that’s not the point of this blog post.  The point here is to state the following:

1. Today, you have N applications in your Portfolio
2. A subset (maybe 100% and maybe a smaller percentage) of those applications and their data must be compliant by the applicable date(s) for your business
3. Every business that is beholden to the mandates needs to list the applications (and data in their portfolio) and then decide which applications (and data) are in-scope. Many companies will do that rapid assessment on their own.  Other companies will enlist the help of partners/vendors to help them move faster and more confidently.  Either way is fine.  If you need a partner to help you move quickly and confidently, we would love to earn that opportunity: contact us at [getfit@cloudfitsoftware.com](mailto:getfit@cloudfitsoftware.com)

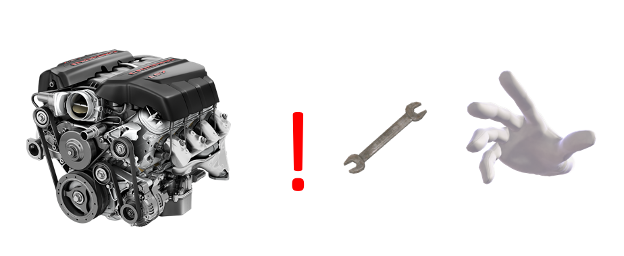
Chart

Description automatically generated

Once you have the list of apps (and data) that are in-scope for you, then what?  Then, it is time to choose an option.

Option 1: Work on the running engine

The challenge with working on a running engine is the increased risk of losing a finger .  Honestly, if you had to spend time quantifying your Portfolio, then it stands to reason that there may be things that you missed in that assessment.  But leaving that point aside, there is always the option to assess every app, every piece of data, every server, every switch, etc to become compliant.  That is a very difficult journey because of years of technical debt.  Can you really clean out all shared-credential-service accounts in your environment without breaking something critical?



Option 2: Build a new engine and rapidly move to it

Surely there are exceptions, but we have yet to see one.  The best answer [is usually] to build a new engine.  Not only is the right answer to build a new engine, but the right answer is to build a new engine in the cloud.

Why the cloud?

1. They are already compliant (e.g. Microsoft Azure Government [MAG] and Government Commercial Cloud [GCC])
2. You will not invest more in cyber and compliance than Microsoft Cloud will, so they are and will be, more secure than you can be
3. If you leverage the cloud, you then only have to worry about securing the pieces and parts that are unique to YOUR business: your enclave(s) and tenant(s), your application(s), your data.

Diagram

Description automatically generated

Executing on Option 2 (New, Cloud Engine)

Step A: Rapidly Establish Cloud Enclave

1. M365: Commercial and/or GCC and/or GCC-High and/or GCC-DOD
   1. Which one(s) do you need?
   2. How do you rapidly set them up and harden them?
   3. How do you continuously monitor (and automatically respond) to anomalies that would take you out of compliance?
   4. How do you give the auditor a real-time dashboard to speed up the audit(s)?
2. Azure: Commercial Azure, Azure Government as IL2, Azure Government as IL4, Azure Government as IL5, or a combination
   1. Which one(s) do you need?
   2. How do you rapidly set them up and harden them?
   3. How do you continuously monitor (and automatically respond) to anomalies that would take you out of compliance?
   4. How do you give the auditor a real-time dashboard to speed up the audit(s)?
3. For every enclave and/or tenant, how will it be managed on Day 1? Day N?  (often, the goal is to “manage it myself” on Day N, but folks are unclear and aren’t ready to manage it on Day 1)

Step B: Move Applications (and Data)

1. How do you prioritize your applications based on timelines and resourcing?
2. For each application, should it
   1. Lift and Shift?
   2. Have slight tweaks? (e.g. converted to PaaS? Converted to hardened containers per DevSecOps Reference Architecture and DoD Standards?  Other?)
   3. Rewrite?
   4. Other?
3. For every application (and data), how will it be managed on Day 1? Day N?  (Often, the goal is to “manage it myself” on Day N, but folks are unclear and aren’t ready to manage it on Day 1)

Step C: What about Client Devices?

1. Are your laptops and desktops managed in such a way that they are compliant?
2. What about mobile devices?
3. Can you detect and minimize spillage?
4. Do you understand your Data Loss posture?

Step D: What about Policies?

1. For example, is your Data Loss Prevention Policy where it needs to be for CMMC?
2. Are the written policies tactically implemented for the Enclaves, Tenants, Apps and Data defined as you establish the enclaves and move the applications?

Step E: What about Auditability?

1. When the auditor shows up, will you spend days and weeks with them, or will you show them your real-time dashboards?
2. When the auditor shows up, will you do tabletop exercises with them? Will you introduce an out-of-compliance-server and watch the automation turn off the server?  Will automation also create a security incident in parallel?  Is it true that the only way to end up with an errant server in this new, pristine engine is that someone went around the process as defined by the policy?’

Surely, you will choose Option 2.

Insource, Outsource or Hybrid?

Now, the only remaining question is whether you will **figure it all out on your own** or will you **bring in someone to help you**?  Given the impact of getting it wrong and given the timeline, most companies will bring in someone to help them.

Which Partner?

There are two courses of action:

1. Pay someone to “consult” with you while doing the work yourself
2. Pay someone to do it for you including Day 1 thru Day N management

Most companies prefer B, but they assume that there is no such unicorn.  And, if they assume there is a unicorn, they fear that they cannot afford it.

What if there were a partner that would come in and do the following:

1. Rapidly define the in-scope apps and data
2. Ask a series of repeatable business questions
3. Rapidly establish the enclave(s) and tenant(s)….using automation within their patented, accredited management platform
4. Rapidly move applications and data to the new enclave(s) and tenant(s) while making the necessary application tweaks and even being willing to take accountability for full application re-writes as necessary….using automation within their patented, accredited management platform
5. Manage the clients and mobile devices and/or work through and with your existing client/mobile team to take accountability for the client and mobile posture ….using automation within their patented, accredited management platform
6. Manage the enclave(s), tenant(s), applications and data to keep them current and compliant….using automation within their patented, accredited management platform
7. Work through and with your Policy team(s) to update Policies as necessary to match the actual implementation
8. Stands at the ready to host your auditors when they show up….using automation within their patented, accredited management platform

Logo, company name

Description automatically generated

* What if that partner also does this same work within DoD?
* What if that partner also does this same work across every industry and vertical *including*for the Cloud Providers themselves on which you will be running?
* What if that partner also does this work for small customers with 5 users as well as for giant customers with over 1M users?
* What if that partner will take accountability for the outcome via a Firm Fixed Price (FFP) contract that is HALF (or LESS) of what you would pay consultants to simply “talk” in course of action 1?
* What if that partner will give you the FFP for the out-years on day 1?
* What if that partner will guarantee that the out-year-pricing stays flat from year 1 thru N?
* What if that partner will give you significant FFP discounts based on how many years you sign up for on day 1?

That partner might sound too good to be true, but it is true.  CloudFit Software IS THAT PARTNER.  See the “Why is CloudFit Software discussing this topic?” section above.

If you want to get started (or if you think we are too good to be true), contact us at [getfit@cloudfitsoftware.com](mailto:getfit@cloudfitsoftware.com) and give us a shot to earn your business.

Filed Under: [Uncategorized](https://www.cloudfitsoftware.com/category/uncategorized/)