The Certification Mindset

For Cloud Service Providers

CoSo Cloud

A CLASS COMPANY

cosocloud.com

The Certification Mindset

For Cloud Service Providers

I'm Rob Porter, Head of Market & Business Development at CoSo Cloud, a firm built on its ability to offer secure eLearning services to customers as demanding of total security for high-consequence learning platforms.

In this guide, I'll take a deep dive into the CSP compliance and information security landscape and show you how the process for pursuing, achieving, and maintaining key certifications plays out in practice.

Most importantly, I'll show you how to approach certifications from a perspective that'll allow you to maximize their benefits to your business while avoiding the black holes of time and money that security certifications are fraught with.

— *Rob Porter*

Head of Market & Business Development
CoSo Cloud

Compliance:

Even more important than you may think

If you're a Cloud Service Provider (CSP) planning on remaining solvent, Information Security and compliance are more important for you than they are for most other organizations: The slightest chink in your armor can allow attackers to ruin your business and your customers' businesses in a minute. Even worse, depending on your offerings, you may not have any business at all without at least some certifications or authorizations proving your security posture.

It's safe to say CoSo's business is wholly dependent on getting security certifications right, and it's my job to make sure we adopt and maintain the right certifications to meet our customers' needs while avoiding the time and money black holes security certifications are fraught with.

There's a lot of nuance in this space and there's almost always more you'll want to consider than simply which certifications meet your needs on paper.

Certifications aren't cheap or easy to achieve and are onerous to maintain, so it's critical to make good selections from the start.

Compliance is an Asset:

How to see it as one

Assets vs. liabilities

Later in this guide, we'll take a look at each of the major certifications and how they might benefit or hinder your business. First, we must discuss getting into the right frame of mind for being a wise shopper of the asset compliance is.

One of the first and most important things you'll find in a business book is the importance of assets versus liabilities: Big single-family houses tend to maximize liabilities: in spite of their higher sale prices, they incur more debt and cost more money to own. Spending the same money on a multi-family home, or maybe a smaller home with a rentable studio maximizes assets. It has the potential to pay for itself, freeing funds for investment and eventually even a bigger house down the line.

Information Security and compliance can work in a very similar way. As the security manager for a CSP, I know that my program funding relies on the products our company sells, so it's in my best interest to do what I can in my domain to increase profitability by maximizing our security program as an asset and limiting the liabilities it poses to the business.

Ignore the hardwood floor

In short, it behooves CSPs to keep their proverbial nut small, which requires approaching compliance decisions smartly, ignoring the granite countertops and hardwood floors and focusing on the economics.

The Economics

Of Compliance Certifications

Every certification gained has at least some value, but that doesn't always mean they're worth the time and money used to achieve and maintain them.

Be thrifty—not cheap

As with nearly every asset, additional certifications will always bring some value to your business. Clearly though, working to achieve and maintain as many as possible or pursuing a particular certification more for its glamor than for the economics can begin to push your compliance efforts from the asset sphere into the liability sphere.

The trick is to know the audience of your offering and get certifications that are cited as requirements for would-be customers.

On the other hand, focusing too strictly on minimizing certifications to the bare minimum required to do business can cut off opportunities. Most CSP security programs tend to start and end at achieving and maintaining only the most crucial certifications. The work required to maintain certifications is quite difficult, and often neither the security team nor the decision makers see growing the business as a security responsibility.

It takes an exceptional security team with exceptional company support to reach out and expand the security program past the minimum viable product and into new (and potentially lucrative) compliance arenas.

This is the classic difference between spending thriftily and simply being cheap, and it certainly applies to compliance certifications. The bare minimum is the bare minimum—seeking certifications beyond that point should always be a calculated growth decision for the business.

The Certification Smorgasbord

With a certifications-as-an-asset perspective in mind, let's dive into the most common certifications and the roles they play for CSPs and their customers.

1. SOC 2 Type 2

This one is pretty standard for North American CSPs and covers basic system-agnostic security controls across numerous domains.

SOC 2 Type 2 isn't the most expensive certification but is highly demanded by customers. Like all certifications on this list, make sure you meet the requirements before you book a CPA to test them, or you're just wasting time and money.

2. HITRUST

Similar to SOC 2 Type 2 but with more controls and as much as twice the overall cost (I do hear they're releasing a cheaper product soon, however).

HITRUST's biggest claim to fame is that it aligns with HIPAA requirements, so this one is marketed to CSPs with health-related clientele.

The Certification Smorgasbord

3. FedRAMP

If your offering is enticing to Federal, State, or local U.S. governments, FedRAMP is for you. FedRAMP certifies providers for one of three "Impact Levels:" Low, Moderate, and High. Most companies strive to reach at least FedRAMP Moderate if they can, but that's not easy. Currently, Moderate has 325 controls to meet and dozens of long documents to write. It's no wonder many companies pay consultants hundreds of thousands of dollars to get them FedRAMP ready. If done without specialist consulting, completing this process will take years and cost the same hundreds of thousands (in some cases, even millions).

Even after all that work and investment, initial assessments still come with an assessment fee of more than 100,000 dollars, which isn't refunded if you fail. For these reasons, security programs with FedRAMP experience are worth their weight in gold.

Fortunately, there's a much faster and cheaper option for organizations that don't want to go it alone or hire expensive consultants. If the conditions are right, it's feasible and far easier to leverage an already authorized company to push your product into FedRAMP at an accelerated pace.

CoSo Cloud is a FedRAMP certified provider that has had an amazing amount of success doing just that.

4. StateRAMP

StateRAMP is a new name in the area and is required by an increasing number of U.S. State-level governments. StateRAMP has a good deal of overlap with FedRAMP, making it very backward compatible, but with a somewhat easier barrier to entry if you aren't FedRAMP authorized. In spite of the lower barriers for StateRAMP, it's better to reach FedRAMP first if possible.

The Certification Smorgasbord

5. DoD CC SRG

IL4 is a word I've been hearing a lot: As the security manager at one of fewer than 50 companies (at the time of this writing) to achieve IL4 or higher, I can tell you that there's a reason so many agencies are pushing for it.

The Department of Defense Cloud Computing System Requirements Guide (DoD CC SRG) is similar to FedRAMP in a few ways: The biggest one is that they use the same security baseline controls starting at the FedRAMP Moderate level, which is known as IL2 in the SRG. There are three other levels to the CC SRG; IL4, IL5, and IL6 (IL3 was absorbed into IL4), that add additional controls with the end goal allowing higher classification of data to be used in the system, as seen in the chart below:

UNCLASSIFIED

DISA — Key Security Requirements Summary

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

The Certification Smorgasbord

6. HIPAA

The Health Insurance Portability and Accountability ACT (HIPAA) is more of a law than a certification. Because there's no certification, your security team needs to be very careful to ensure you are compliant. I've heard some auditors claim that over 90% of HIPAA audits fail.

Violations of HIPAA can end in fines, some of which have penalties ranging from 10s of thousands to millions of dollars. That being said, healthcare and healthcare-adjacent companies require HIPAA compliance, in some cases even when the offering has nothing to do with Personal Health Information (PHI).

7. GDPR

General Data Protection Regulation (GDPR) is an EU law concerning the privacy of personal data. This is another scenario where self-assessment is possible but getting it wrong can have significant consequences.

GDPR is a must-have for European CSPs, but it's my opinion that any CSP anywhere should try to reach compliance if possible, or you're excluding yourself from a large market.

FedRAMP High vs. IL4-6:
What's more secure?

This is a question that comes up quite frequently and deserves its own discussion.

There's not really a continuum of security in this space: Beyond FedRAMP Moderate/DoD IL2 there is some deviation in purpose.

The way I like to think about it is that FedRAMP High is there to boost overall security posture of the environment by adding about 100 new general security controls to the baseline, where DoD IL4 and above act as an overlay of controls on top of the FedRAMP to focus more on specific controls necessary to connect to the DoD network and monitoring services, as well as additional controls surrounding security and handling of the data in the environment itself.

It's possible to have any combination of FedRAMP Moderate or High along with IL4-6 depending on the use case, but there must absolutely be a use case; any DoD authorization must come with a DoD agency sponsorship, and your authorization level must meet their needs.

FedRAMP High vs. IL4-6:
What's more secure?

So what's the difference exactly?

Where FedRAMP focuses on general security posture, DoD focuses on data privacy and general controls meant to prepare your system for being introduced to the DoD network. DoD certification adds an additional layer of data privacy controls on top of FedRAMP baselines.

The controls in IL4-6 are additional requirements that are mostly focused on data security rather than overall security posture. There are also quite a few additional controls to handle "General Readiness", which are meant to prepare your system to be included in the DoD network.

FedRAMP High vs. IL4-6:
What's more secure?

So you want to pursue IL4

As I mentioned earlier, CoSo is one of only about 50 companies to have achieved IL4 or higher, despite agencies' increasing interest in working with companies that have achieved it.

The reasons for this difficulty are several:

1. Stringent security requirements: IL4 authorization requires a high level of security, including physical, network, and system security, and strict incident management and reporting protocols. It can be challenging for organizations to meet these requirements and maintain compliance.

2. Complex and lengthy process: The process of achieving IL4 authorization is complex and can be time-consuming. It typically involves a comprehensive risk assessment, development of security controls and procedures, and an on-site assessment by an accredited third-party auditor.

3. High costs: The process of achieving IL4 authorization can be costly, including the cost of implementing and maintaining the necessary security controls, as well as the cost of the assessment itself.

FedRAMP High vs. IL4-6:
What's more secure?

So you want to pursue IL4

4. Limited number of accredited assessors: There are a limited number of third-party organizations that are accredited to conduct IL4 assessments, which can lead to delays in the assessment process.

5. Regular audits and assessments: Even after achieving IL4 authorization, organizations must continuously maintain and demonstrate compliance through regular audits and assessments.

6. The IL4 standard is only intended for systems or services that process sensitive information, such as personal data, and government information and the bar is set high to protect that kind of information.

In summary, achieving IL4 authorization can be a complex and challenging process, requiring a significant investment of time, money, and resources. It is essential that organizations thoroughly understand the requirements and are prepared to commit to ongoing compliance efforts.

If and when IL4 does make sense for your business and customers, achieving and maintaining it could be a major asset.

Further Considerations

When you're doing security well, you're in a position to help others as a Managed Security Service Provider (MSSP).

Security-as-a-Service

if your CSP has a mature security program, it may be possible to sell those services as a Managed Security Service Provider (MSSP). You've already paid for all the security staff and tools to protect your own environment; why not protect others?

Services rendered can range from network monitoring and ConMon to consulting services for policies, procedures, authorizations, etc.
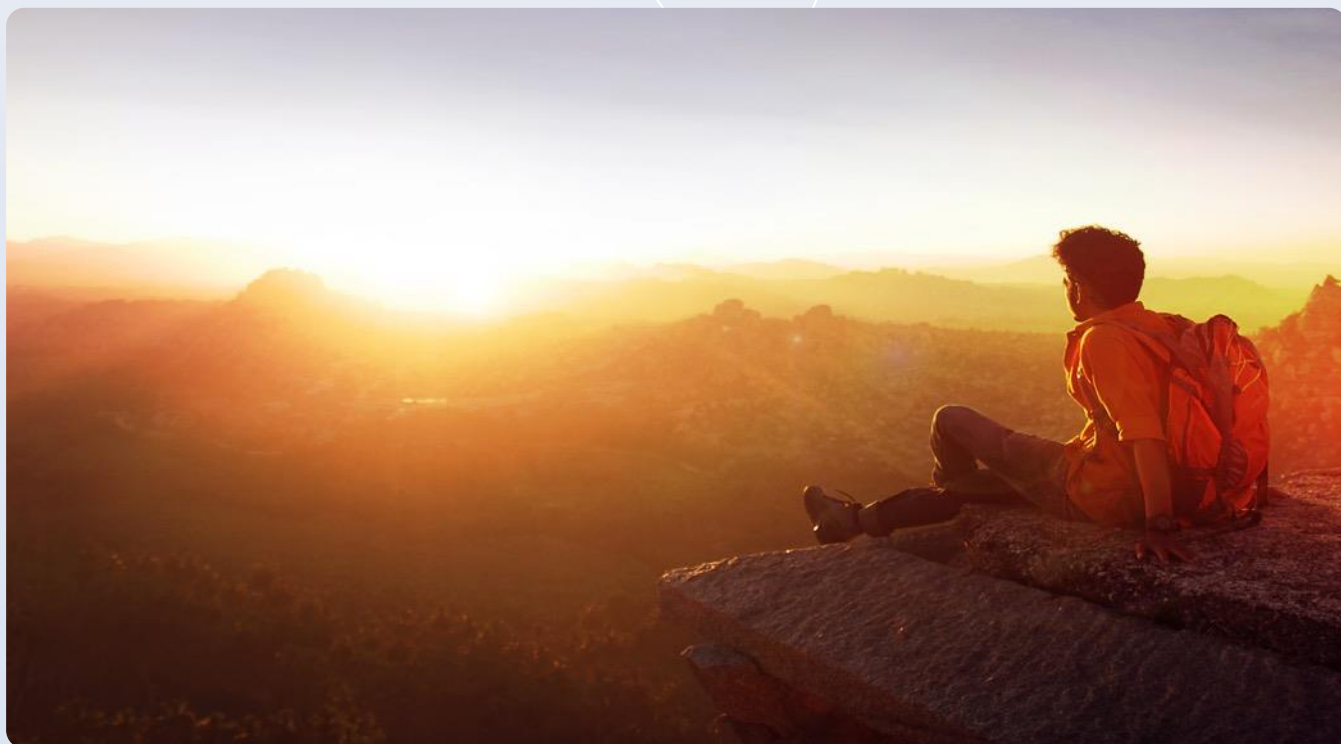
If You Build It, Will They Come?

Maybe not. It's important to note that some authorizations may cost more than they're worth to your customers, and some may not even be possible without existing interest. If you don't have any U.S. government customers asking about authorizations such as FedRAMP, you should ensure your offering is useful in government use cases before pursuing it.

Regarding some of the more difficult authorizations like FedRAMP High and even IL4, there is a considerable additional cost in technology to meet the new security controls required and a much higher yearly audit cost to have the controls tested.

Having FedRAMP High is undoubtedly a feather in the cap to prove you've got a well-secured platform (and IL4 puts a firm in a super elite class), but it might not improve overall value if your offering doesn't meet high-security use cases.