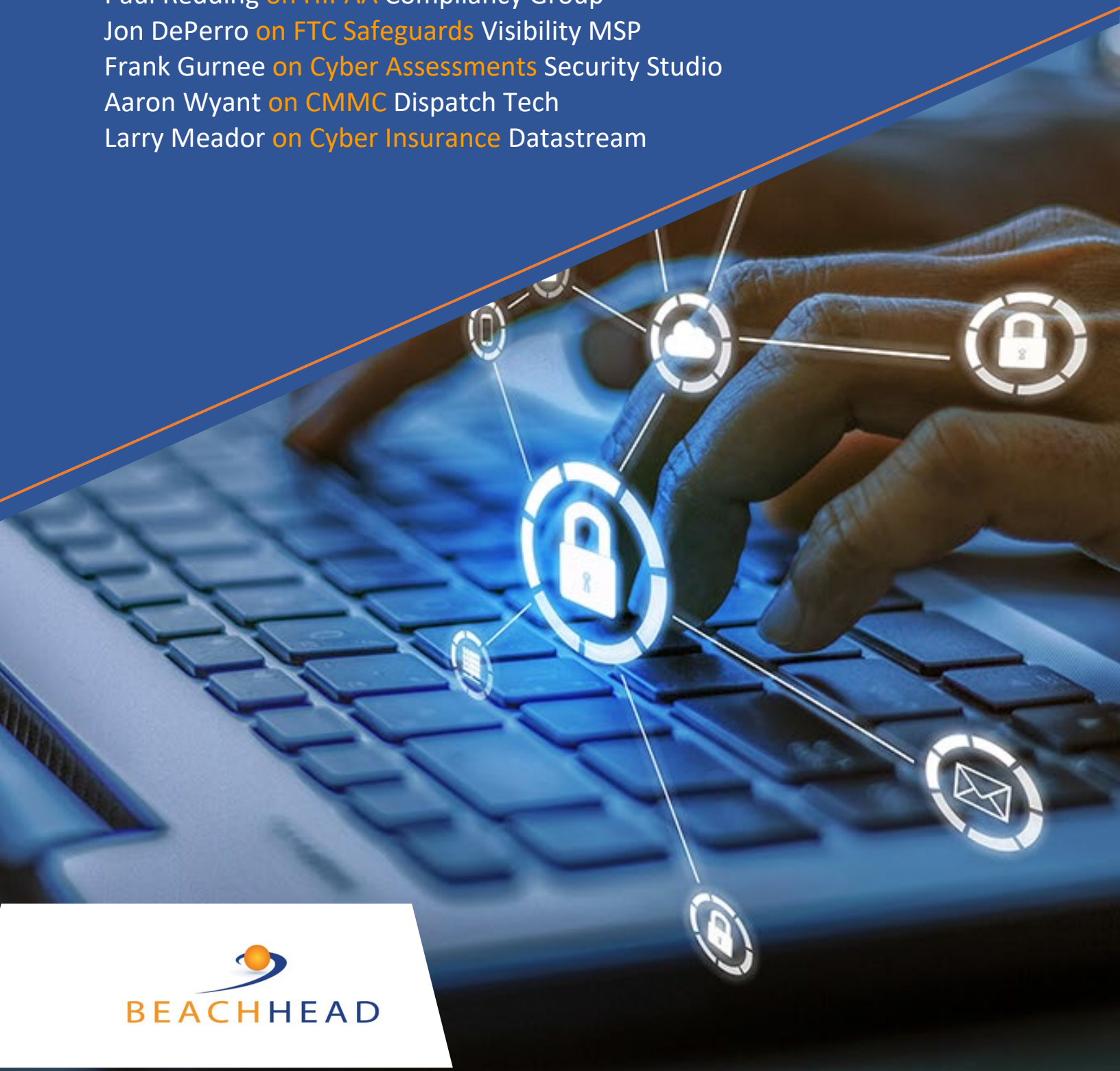
2024 Industry Report

MSP Guide to Compliance And Regulation

Use to Win and Maintain Business!

With contributions from:

Paul Redding on HIPAA Compliancy Group
Jon DePerro on FTC Safeguards Visibility MSP
Frank Gurnee on Cyber Assessments Security Studio
Aaron Wyant on CMMC Dispatch Tech
Larry Meador on Cyber Insurance Datastream



BEACHHEAD

In no uncertain terms: compliance is coming for you and your clients

Regulatory compliance is unavoidable no matter what types of clients your MSP practice works with—hard stop. But this white paper can help you not just highlight what you need to know right now across several key compliance mandates, but also delivers won't-find-it-anywhere-else peer insight to advance your practice *because* of compliance.

Perhaps your firm has intentionally sidestepped dealing with clients in strictly regulated sectors like healthcare or financial services, preferring to target less regulated industries with fewer stringent requirements. You might reason, "There's an abundance of businesses out there without such strict security and access control guardrails; they don't require compliance, so why should I?" However, sooner or later (and at this point, it's really just *sooner*), every company in America will need to adhere to some form of regulatory control. Ditto to avoiding cybersecurity insurance, a decision that will increasingly put an MSP practice's survival at risk.

We get it: navigating the labyrinth of regulatory acronyms and industry-specific requirements may seem overwhelming. But it's not all bleak. There is, in fact, more commonality among these mandates than you might think. Some of the terms swimming around in your head are simply guides, while others represent certifications you or your clients might need.

In order to demystify this evolving landscape, we've assembled a team of expert and highly regarded voices within the MSP ecosystem. Their insights have been crucial in helping us comprehend these complexities. In lieu of further complicating matters by attempting to self-educate through countless Google searches, these experts offer reliable, current, and first-hand knowledge.

We believe this Guide may help eliminate some of the confusion and provide a roadmap for action.

Read on to learn how you can protect your MSP practice, safeguard your clients, offer advice, and use compliance expertise to win more business.

FTC Safeguards: A Primer

Jon DePerro, Chief Compliance Officer at Visibility MSP

The FTC Safeguards Rule requires businesses that act as a "financial institution" to maintain an information security program that can effectively keep customer data secure and confidential. Critically, the term "financial institution" broadly applies to any business (under FTC jurisdiction and not that of another regulator) involved in transferring money to and from customers. This means that millions of businesses potentially must comply: the Rule itself names 13 example entities that qualify, including mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors, and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors, and finders.

The FTC Safeguards Rule requires a written information security program appropriate to the size and scope of the business, its activities, and the sensitivity of the customer information it handles. The Rule also defines nine required elements of an acceptable information security program. First, a business must designate a qualified individual to implement and supervise the information security program, who can be an internal employee or an MSP professional. Second, a business must conduct a written risk assessment that inventories customer information and evaluates threats (and must reassess risks whenever operations or threats change). Third, a business must introduce safeguards aligned with the risk assessment, including access controls, data encryption, multi-factor authentication, secure data disposal, activity logs, and more. Fourth, a business must conduct continuous security testing (or regular pentesting and vulnerability assessments). Fifth, sixth and seventh, a business must introduce employee security training, monitor service providers to meet security expectations, and keep its information security program updated to current needs.

What To Do

The ubiquity of the FTC Safeguards Rule is quickly becoming apparent—and urgent—to the countless businesses under its purview. While major enterprises with well-paid cybersecurity experts on staff are ready to adapt, many SMBs will increasingly seek out MSP expertise as their most realistic means of complying with the law.

Already, businesses are asking their MSPs to provide the security protections the Rule requires, and if they cannot, they'll switch to an MSP that can. From a competitive perspective, MSPs would be wise to add assistance with FTC Safeguards Rule compliance to their services. That compliance is not optional: affected businesses put their licensing in jeopardy if they fail to meet the Rule's requirements. MSPs that offer that compliance will encounter frequent opportunities to gain clients and capture business from competing practices; those that don't will see clients move on.

In addressing potential clients, MSPs can thrive by making the stakes clear. The FTC Safeguards Rule has particularly big teeth. A business can face a $100,000 fine per violation. Additional fines can hit a business's officers and directors individually. For example, CEOs who are not directly responsible for security can nevertheless receive fines—thus making FTC their responsibility, too. MSPs should let potential clients know that ignorance isn't protection, but the right MSP partner is.

A Deeper Dive with Jon

1. *Are the requirements of the FTC Safeguards Rule here to stay?*

I've spoken with business owners and colleagues harboring the misconception that the teeth of the FTC Safeguards Rule depends on which political administration is in charge. Maybe it is wishful thinking that their laziness will pay off and not come to bite them. That notion is simply false. The Rule is here to stay, no matter who's in office. It's true that the Rule is subject to revision, and businesses and MSPs better keep up with the latest. But it's only going to get stricter over time. Anyone betting on ignoring it is due to come out on the losing end if they don't get with reality, and quickly.

2. *When do businesses need to get compliant with the FTC Safeguards Rule?*

Yesterday. The Rule came out in 2021, with an original deadline to get compliant by December 2022. After some lobbying and complaints that there weren't enough security experts in the world to get all these companies prepared in time, that deadline got kicked back to June 2023. Well, that's now in the past. If your business isn't ready yet, you're already exposed and at risk of FTC fines. So, the answer to when do businesses need to comply by is ASAP.

3. *What opportunities does the FTC Safeguards Rule offer for MSPs, as opposed to CMMC?*

In my opinion, FTC Safeguards offers a more advantageous focus for many MSPs' businesses. The FTC Safeguards Rule requires "non-banking financial institutions" to implement comprehensive security around customer financial data. "Financial institutions" is broadly defined as any business that regularly transfers money to and from customers. We're talking about millions of businesses: real estate attorneys, car dealerships, roofing companies, etc. That's a massive audience, and the types of companies the average MSP already works with.

For MSPs, CMMC projects may pay out in the mid-six figures, but you need to hire a team of experts where the junior employees are pushing six figures themselves. And, a single CMMC project will eat up 20 hours a week for six months. Do you have the bandwidth to handle that project and run your MSP? Meanwhile, FTC Safeguards is already in an MSP's wheelhouse. MSPs prepared for FTC Safeguards are also better positioned to move toward CMMC down the road if they like.

4. *For MSPs, what's the impact of preparedness for the FTC Safeguards Rule—or really any compliance framework—from a competitive standpoint?*

MSPs that don't understand compliance, whether that's NIST, HIPAA, etc., will increasingly lose customers to those that do. An MSP prepared for FTC Safeguards can approach a prospect and say, "Your IT doesn't meet your needs, why doesn't your current MSP have you ready? The FTC, your credit card company, and your cyber insurance company all have requirements or contractual obligations you aren't meeting. We can make them all happy." Say that, and you can steal a client's full business away from their previous MSP. Delivering demonstrable security against the FTC Safeguards Rule is a big advantage right now.

About the Contributor

Jon DePerro

Chief Compliance Officer at Visibility MSP

Jon has over two decades in security and risk management. Most of this time was with the US Army where he served as a Counterintelligence Special Agent. Jon's various global assignments involved advanced security and threat management roles at the Army's Intelligence and Security Command and the NSA in support of the national intelligence and US Special Operations communities. He was also selected to serve as a founding member of NATOs first ever military cyber-defense working group.

Jon has spent the past three years working with MSPs to help them understand security, compliance, and risk management. His guiding work principle is security and compliance should enable business operations by allowing senior leaders to make informed risk decisions while protecting critical business functions.

Your HIPAA Primer

Paul Redding, Vice President
Channel, Engagement & Cybersecurity of the Compliancy Group

Arguably the bellwether of modern IT compliance, HIPAA—the Health Insurance Portability and Accountability Act—was enacted in 1996 to protect patients' sensitive health information. Compliance with HIPAA is essential to safeguard patient data and avoid potential legal and financial penalties. With many small and mid-size healthcare delivery organizations turning to MSPs to ensure HIPAA compatibility, MSPs must have a firm understanding of the law's requirements and their role in assisting clients.

That understanding starts with Business Associate Agreements (BAAs). HIPAA applies to "covered entities," including healthcare providers, health plans, and healthcare clearinghouses. Because MSPs have the ability, in most instances, to access HIPAA Covered Entities' (CE) protected health information (PHI), the MSP must comply with HIPAA's regulations—which means signing BAAs and adhering to the Security and Privacy Rule. The latter sets specific requirements for safeguarding PHI. The security section outlines three types of safeguards that covered entities and MSPs must implement to protect electronic PHI (ePHI): including administrative safeguards (such as risk assessments and workforce training), physical safeguards (such as access controls and facility security), and technical safeguards (such as encryption and security software). The privacy section, on the other hand, outlines the permissible uses and disclosures of PHI. This rule requires that covered entities and MSPs obtain written authorization from patients before disclosing their PHI, except in cases where the disclosure is for treatment, payment, or healthcare operations.

What To Do

MSPs must perform regular risk assessments to identify potential vulnerabilities and risks to patient PHI. This is an essential part of HIPAA compliance and helps covered entities and MSPs understand their security posture and identify areas that require improvement. The risk assessment process involves identifying potential threats and vulnerabilities, assessing the likelihood and impact of those risks, implementing measures to mitigate those risks, and fully documenting this process.

In the event someone does go awry, MSPs must have an incident response plan in place to address security incidents or breaches. The plan should outline steps for investigating and responding to security incidents—including reporting to the covered entity and affected individuals, as required by HIPAA. An incident response plan is crucial to minimizing the impact of a security incident and preventing similar incidents from occurring in the future.

MSPs must also provide training and awareness to their employees on HIPAA compliance and security best practices. This includes training on how to handle PHI, the importance of safeguarding PHI, and how to identify and respond to security incidents. Regular training and awareness programs can help MSPs reduce the risk of security incidents and ensure that their employees are aware of their responsibilities under HIPAA.

MSPs are critical in helping healthcare organization clients achieve and maintain HIPAA compliance. But to do this, MSPs must be familiar with the requirements of HIPAA and understand their role in assisting their clients. MSPs must sign BAAs, adhere to the Security and Privacy Rule, perform regular risk assessments, have an incident response plan in place, and provide training and awareness programs to their employees. Compliance with HIPAA is essential to safeguarding patient data and avoiding legal and financial penalties for healthcare organizations.

A Deeper Dive with Paul Redding

1. *What is the relationship between NIST and HIPAA?*

HIPAA borrowed from early frameworks like ISO and NIST, but it predates CSF and other current cybersecurity frameworks. That said, HIPAA can be mapped to NIST CSF, ISO 27001, and other modern standards. Under the recent bill, H.R.7898, healthcare organizations are now allowed to use these mappings to align their security policies to these more robust control sets.

2. *What do MSPs need to know about the HICP guidelines?*

This is the "you should" part of HIPAA. Originally drafted in 2005, they just released a major overall to the 405(d) HICP guidelines. One of the most interesting components is that there is now *guidance for how healthcare providers can and should choose an MSP partner*. It's a huge departure from the past, where HIPAA was written more with more of a "you can do this by yourself" conclusion for healthcare organizations. But the guidelines have since become so complex and the threat landscape has changed so much that there's now an assumption that it's not reasonable for smaller healthcare practices to do this all themselves. It is much more prescriptive healthcare control.

3. *How concerned do I need to be about HIPAA fines and enforcement?*

Very. HIPAA fines used to be practice-crippling. Fines were in the millions of dollars, and healthcare organizations were more or less under the mindset that a HIPAA violation was probably rare…but if it happened, it would kill their business. But now you're starting to see fines that more realistic—in the $35,000-$50,000 range per violation. These are no longer bankrupting sums, and violators are expected to pay. You are going to see more and more enforcement. Think about it in a way kind of similar to ransomware: smart attackers ask for a sum that they know will be more likely to be paid, versus a number where you have no realistic choice but to give up your data. It's a hard lesson that is coming for healthcare practices, but one that should make MSPs' value as a HIPAA compliance expert that much more critical.

About the Contributor

Paul Redding

Vice President of Channel, Engagement, & Cybersecurity of the Compliancy Group

As the former CEO of an MSP, Paul has an extensive background in cybersecurity. Throughout the years, Paul has advised multiple healthcare organizations on the security measures they needed to have in place to protect their information and be in compliance with HIPAA. As the VP of Channel with Compliancy Group, Paul works with technology service provider partners, advising them on how HIPAA compliance can benefit their business. He takes his knowledge to the trade show stage, educating MSPs on the importance of compliance, and how they can simplify compliance for their clients.

Your Cybersecurity Assessment Primer

Frank Gurnee, Channel Director, Security Studio

Effective cybersecurity assessments take a comprehensive look across an organization's systems, networks, processes, and controls to flag recognized risks and vulnerabilities and suggest recommended security enhancements. MSPs and their clients operating in industries governed by regulatory compliance frameworks must adhere to strict requirements designed to safeguard sensitive data, and cybersecurity assessments provide that requisite snapshot evaluation of security posture.

If an MSP or their client is lacking sufficient technology or processes, assessments will point to the improvements required to align practices with compliance requirements. Many MSPs will find they have a significant opportunity to utilize cybersecurity assessments to provide clients with expert guidance in securing their data and IT infrastructure, while also preparing clients for potential vetting via regulatory audits or cybersecurity questionnaires that their own clients may require.

To conduct comprehensive cybersecurity assessments, MSPs must have deep expertise and technical capabilities for conducting risk assessments, compliance assessments, vulnerability assessments, penetration testing, and assessments of security controls, governance, employee-based risks, third-party risks, and other emerging threats. Compliance assessments require close familiarity with key frameworks such as NIST, HIPAA, GDPR, and other standards pertinent to an MSP's individual clients. Vulnerability assessments and penetration tests identify network, system, and application vulnerabilities, enabling MSPs to recommend and execute needed remediations. Security controls such as network security, access controls, endpoint security, data protection, and incident response must be assessed to ensure their effectiveness and inform MSPs where they should plug any gaps. Assessments of employee security awareness and risks will reveal if more robust security training regimens are necessary. Clients' third-party relationships must be assessed for risks as well. Finally, cybersecurity assessments must account for newly emerging threat practices and attack vectors, requiring MSPs to continuously evolve their security knowledge and proactive apply those learnings.

What To Do

It is critical that MSPs go beyond just checking off boxes. Instead, they ought to wield cybersecurity assessments as part of their holistic approach to risk management and risk reduction. Accurate assessments and MSP-led remediation helps clients drive down the cost of compliance and, more importantly, flips security from a pain point into an asset able to drive business development and marketplace differentiation.

When engaging with any new client, MSPs should first conduct a risk assessment to determine the correct start points for addressing their security and compliance needs. As a best practice, MSPs should also apply the same assessment processes to their own practice. Not only does doing so enable subsequent security hardening, it also allows for more hands-on experience with key solutions. And when clients ask MSP representatives if they use the same procedures internally, they can say "yes."

Next, it's crucial to help clients understand cybersecurity assessments from the perspective of business value versus IT value. For example, while an older laptop may have depreciated in value to where the hardware is only worth a few hundred dollars, the business value of securing that device and the sensitive data on it may be closer to priceless. Security investments are not an IT value conversation—they're about the larger business value. MSPs able to engage clients in those larger conversations lead them to more effective security (as well as additional product and service revenue opportunities for MSPs themselves).

Lastly, MSPs must establish a continuous security relationship with clients that is designed to address continuous risks. A successful security and compliance strategy is like a successful MSP-client relationship: engagements aren't one-and-done. MSPs should make clear that working with them will include ongoing assessments and activities to improve security, reduce risk, and remain compliant.

A Deeper Dive with Frank Gurnee

1. What do clients misunderstand about MSPs and cybersecurity assessments, and how should MSPs clear up those misunderstandings?

Clients often believe that their MSPs conduct thorough cybersecurity assessments at the start of their relationships. But the reality is that many aren't—at all. If you ask those MSPs' clients if they're worried about the latest XYZ vulnerability in the news, they'll say they have full confidence in their MSP and have no worries. The truth, though, is that their MSP often hasn't even considered the risk of XYZ. Most clients simply aren't aware of the risk they're in, and that's not good for them or an MSP's business.

True security-minded MSPs can break through to potential and current clients by clearly demonstrating the difference in their approaches. For example, a smart MSP would never simply throw products at a client without conducting and sharing a comprehensive cybersecurity assessment, because it's essential to first understand what products are actually appropriate and will help the MSP achieve a successful ongoing business relationship. MSPs can and should point out the not-so-subtle differences between checking off boxes and actually delivering effective security. And because MSPs are now rich targets for threat actors as well—since breaching them can mean breaching all their customers at once—MSPs that practice what they preach and use the assessments and tooling they offer internally can demonstrate greater trustworthiness.

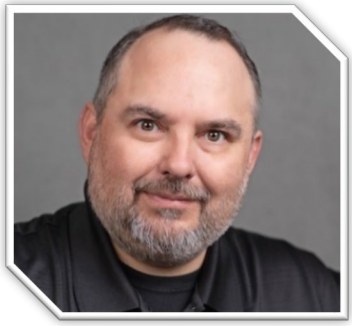
5. What should MSPs know about popular cybersecurity frameworks?

We'll regularly meet a client that says, "We're SOC 2 compliant, so there's nothing to worry about"…only for our cybersecurity assessment to identify all kinds of holes in their security. We then have to explain that SOC 2 is an accounting standard, but it doesn't account for everything businesses need to be secure. The same is true if you look at many cybersecurity questionnaires. They're often overly specific about asking what configuration settings are in place, but the question will only be relevant because several levels up there's a function of risk management and governance that should ensure the correct configurations to prevent a breach.

The bottom line for MSPs is this: there are potential gaps between compliancy and actual security. Cybersecurity assessments that enable an MSP to assess a client's security posture can not only help achieve compliancy, but can also help point out where further attention and new protections are needed. Ultimately, MSPs benefit from helping clients to become wiser and more security-conscious.

6. How should MSPs reset clients' expectations about the cadence with which they address their security profiles?

If a client says they do a security audit once a year, I like to ask, "How often do you think cybercriminals refresh their attacks, once a year?" That changes the conversation. Since attackers are innovating 24/7, businesses should bolster their protections at a frequency to match. "Our security is good once a year" isn't effective enough, and there's always something to work on to become more secure for the next assessment. Effective security is ongoing, and as technology and threat actors change, security-focused MSPs can maintain long-lasting relationships with clients by continuously delivering sufficient protections.



About the Contributor

Frank Gurnee

Channel Director at Security Studio

Frank Gurnee is an innovative and dedicated professional with over 25 years of experience in the IT/MSP channel. As a key early employee at Covad Communications, he played a vital role in the company's success as a pioneer in broadband. Frank helped form CharTec, an MSP training organization, which has become essential for comprehensive MSP training. His program development expertise led him to Vertical Axion, an MSP-focused Web Marketing company. Currently, as the Channel Director at SecurityStudio, Frank is at the forefront of assisting MSPs in navigating security and risk management, ensuring their continued success in the evolving MSP world.

Your CMMC Primer

Aaron Wyant, President of Dispatch Tech

Organizations within the Department of Defense (DoD) supply chain—*including* all contractors and subcontractors—are subject to the DFARS 252.204-7012 clause and the Cybersecurity Maturity Model Certification (CMMC). The DFARS 7012 clause states that any organization with a DoD contract or subcontract storing, processing, or transmitting controlled information must protect that information in accordance with the NIST special publication 800-171 framework and additional requirements.

The DoD introduced the current version of CMMC (CMMC 2.0) in November 2021 to better enforce cybersecurity via third-party assessment and certification. With 2.0, CMMC now has three different levels of cybersecurity requirements (down from five) representing increasing maturity and controls. The type of information a contractor or subcontractor handles determines the CMMC level that the organization is required to achieve. Organizations are subject to examination by a CMMC Third-Party Assessment Organization (C3PAO)—an independent and accredited entity—that will vet an organization's security practices and provide certification if that organization is in compliance with its required CMMC level.

In practice, the odds of an organization undergoing a third-party assessment will be low. However, CMMC also requires organizations to undergo a Basic Contractor Self-Assessment and submit and self-attest to the resulting Summary Level Score, or Supplier Performance Risk System (SPRS) score, in order to be eligible to bid on defense contracts. The SPRS score is based on the NIST SP 800-171 DoD Assessment Scoring Template. A perfect score is 110—and anything less is a failing score. Any organization that scores less than 110 must submit a Plan of Action and Milestones (POA&M) that documents the cybersecurity improvements it will pursue (and projected times to completion). The DoD views this submitted document as a binding commitment to achieve necessary CMMC compliance.

What To Do

MSPs can provide crucial expertise and support in ensuring clients understand their duties under CMMC, navigate assessment processes, and pursue CMMC compliance in order to ultimately win new business. Specifically, MSPs should deliver cybersecurity services that include effective data protection and access controls, thorough and accurate risk assessments, and the other guidance required to meet the technical criteria required by CMMC.

Because CMMC focuses on safeguards that secure controlled unclassified information (CUI)— including personally identifiable information (PII), sensitive technical data, and more—MSPs can serve clients well by introducing security controls that align with best practices for securing this information across their organizations. CMMC similarly calls for all cybersecurity practices to undergo *continuous* monitoring. MSPs should thus provide clients with effective check-and-balance strategies and ongoing security assessments, with a focus on maintaining and assuring compliance with the CMMC framework.

MSPs should also be well aware of the relatively dynamic nature of CMMC, and they should be ready to adapt as trends change that shift CMMC compliance requirements. With the present version of CMMC (2.) set for final implementation by 2025, MSPs must remain on top of new developments, and be ready to adjust client recommendations and security postures accordingly.

A Deeper Dive with Aaron Wyant

1. *How can MSPs distinguish themselves—and win business—with CMMC compliance?*

Number one, if you're just starting out on the CMMC compliance road, find partners that have already been through it. Seek help, and you'll save time, headache, and money. It's a lot of work, and it's specific work. Even if you may *think* your system is CMMC-compliant, you might still need to search for certain tools that can really match to the right purpose. It's a bit of the Wild West of CMMC compliancy right now for MSPs, as they increasingly try to position themselves favorably (and they should). But if you're ill-prepared and want to get it right on your own, it's going to take time—possibly years. But partner with someone that has the experience with CMMC controls, and you fast-track that. Even if you don't currently have a client currently selling to the government, CMMC compliance can be critical for showing your security chops when going after new business. CMMC reflects directly to the NIST 800-171 controls; this is what the government is deciding is just baseline cybersecurity measures, and it's only going to become more important and more table stakes for earning business.

2. *Of the 110 CMMC controls, are there any that stand out as particularly challenging?*

Yes—FIPS validation. There's a complete back and forth from the rulemaking board, from the community, and even from NIST itself on what does that requirement mean. And the reason why is that you can run a FIPS-compliant algorithm (and now it's to that level of security), but then they might want a validation straight from NIST.gov. And what we're finding with certain vendors is that some of them are pursuing that level of FIPS 140-2 validation, and some of them are using FIPS 140-2-compliant algorithms and their software. There's no resolution on this yet, and a complete back-and-forth of people arguing over it.

3. *What is one of the biggest industry misconceptions around CMMC?*

The glaring one is that you get these companies that say they do CMMC, but they actually don't. They say they do, but you're buying a tool that doesn't do anything. It's really important to do your homework on this—the risks are too high. Then, if you are able to successfully get CMMC certification, you're in a good position to then pass cybersecurity insurance questionnaires, or meet ISO 27001 or 800-171 standards. If you're CMMC-compliant, you've shown that you adhere to all the NIST controls, which everything else derives from. But it all starts with having (or finding) the confidence that the path you're on will get you where you need to be. With 110 controls, it can be tricky.

About the Contributor

Aaron Wyant

President, Dispatch Tech

Aaron Wyant, President of Dispatch Tech, Inc., has an impressive background with over 36 years of experience in computer technology. He is the co-author of the Amazon best-seller "On Thin Ice" and the creator of "Operation Success Magazine." In 2008, Aaron founded Dispatch Tech, Inc. What began as a traditional break-fix service quickly evolved into a full-fledged Cybersecurity and CMMC compliance company, thanks to the dedication and excellence of his team. Under Aaron's guidance, the company has flourished, and his current goal is to assist other Managed Service Providers (MSPs) in helping their clients become CMMC compliant.

Your Cyber Insurance Primer

Larry Meador, Channel Chief Datastream Cyber Insurance

Cyber insurance offers businesses protection against the financial impacts of cybersecurity incidents. When a data breach occurs, organizations face (often significant) costs related to the data breach response and subsequent investigation, legal and public relations expenses, and fines from regulators. Having a sufficient cyber insurance policy mitigates these costs and risks.

Why does this Guide devote a discussion to cybersecurity insurance? Often, the requirements outlined in cyber insurance policies—and guidance for the payment of claims—are based on the requirements of compliance mandates. In fact, adhering to the requirements of cyber insurance policies is often a springboard to meeting the requirements of the mandates this Guide details.

Because cyber insurance policies vary widely in the specifics of their coverage and the options available, MSPs and IT service providers play a crucial role in helping clients choose policies that effectively protect their business and understand the requirements of any policies they currently hold. Cyber insurance policies can offer *first-party coverage* for expenses the insured organization itself incurs during an incident, as well as *third-party coverage* that addresses expenses associated with that business's customers (or other parties affected by a breach). Policies can also include sub-limits and exclusions. For example, a $1 million-dollar policy might have a sub-limit and only cover $25,000 for ransomware incidents, or a policy might not cover costs associated with social engineering attacks at all (currently one of the biggest causes of losses). Businesses must also size their policies correctly. A $1 million-dollar policy is insufficient for a business with $50 million in revenue. MSPs should recommend minimum coverage of $1 million and, beyond that, coverage should equate to roughly 15% of annual revenue. So, for an MSP client with $50 million in revenue, they should look at a minimum of $7.5 million in coverage. Further, MSPs should carefully vet all terms and conditions in clients' policies and assist in addressing any mismatches with their needs.

What To Do

MSPs must help clients understand and appreciate the importance of cyber insurance coverage, and they must also ensure that sufficient cybersecurity protections are in place to meet policy specifications. Cyber insurance providers aren't interested in writing blank checks to defenseless businesses: the underwriting process includes a thorough risk assessment and security questionnaire. The cybersecurity protections required by cyber insurance providers drive considerable spending on MSP services. Compliance requirements impacting clients in regulated industries go hand-in-hand with cyber insurance as well.

That said, MSPs must ensure that every cybersecurity protection a policy requires—and that a client attests to having in place—is correctly utilized and thoroughly documented. For example, if a policy requires that all of a client's endpoint devices have multi-factor authentication, the client must take screenshots and collect all other available documentation of those protections. As the client adds devices, it must append its documentation to continually prove its security. When an incident occurs and the insurer sends a digital forensics team to verify the presence of all protections required by its policy, the onus of proof is on the client. The right documentation is the difference between a claim being paid or not. MSPs can support clients by offering tools to simplify the documentation of security measures. MSPs should also provide in-depth incident response planning aligned with insurance provider requirements, and build collaborative relationships with providers to remain aligned with evolving trends, risks, and best practices.

A Deeper Dive with Larry

1. *How are cyber insurance requirements evolving?*

I think that within 10 years or so, cyber insurance will probably be *required* for most (if not all) businesses. You can't own a home without home insurance. You can't drive a car without auto insurance. Eventually, you won't be able to run a business without cyber insurance. That's because a cybersecurity failure can easily wipe out a business. And no business vertical today is immune to that danger. Imagine if a critical infrastructure business got hit and didn't have cyber insurance. That's why you're seeing the government take a more active role in cyber security/cyber insurance. And I would anticipate that after the recent MOVEit vulnerability, that just might be the impetus that accelerates government involvement.

Smart lenders already require small businesses to carry cyber insurance, as they've been burned by companies that shut down after ransomware attacks and couldn't repay their loans. Many third-party contracts now regularly require cyber insurance for partners within the supply chain. Even MSPs are increasingly starting to write cyber insurance requirements into their own managed service agreements to protect themselves. Essentially, they're saying, "If you want to do business with my company, you'll have cyber insurance. Otherwise, it's not worth the risk."

2. *What should MSPs and their clients look for when considering cyber insurance partners?*

Many traditional insurers ventured into cyber insurance pre-pandemic…despite their complete lack of knowledge or cybersecurity expertise. As a result, many businesses obtained cyber insurance from their local agents, thinking they were getting adequate coverage. While that might sound convenient, the scary thing is that we hear horror stories—often—about those providers not paying insurance claims. The reason why is that those local agents didn't properly explain the policy to their customers. Often, this was due to the simple fact that the agent themselves didn't understand what was contained in the policy—and customers wound up without the required protections or documentation when a security incident occurred. Thankfully, many carriers are now much more in-tune with cybersecurity technologies, hence why you now see cyber insurance driving cyber security technology spend.

MSPs can borrow the following analogy to help steer clients to the right providers. A lot of people have a family doctor they like. But if you need open heart surgery, are you going to them? No way. You go to a specialist. It's the same for cyber insurance. Cyber insurance is such a different beast than traditional insurance lines (and you don't want to realize that once you're already on the proverbial operating table). that it truly benefits a business to work with a cyber insurance specialist to make sure you are adequately covered.

3. *How can MSPs help clients frame a successful approach to cyber insurance?*

The fact that the media only covers huge data breaches is a huge challenge for MSPs, because it makes small- and medium-sized businesses (SMBs) think they're immune to cyber threats. The reality is that hundreds of security incidents are targeted at SMBs each and every day. They just don't make the press, simply because a small business getting attacked isn't as newsworthy as a Colonial Pipeline or a Target. The scary truth is that bad threat actors have learned that it is actually easier to target smaller businesses (with typically weaker security postures) than to *try* to rob big fish that they know will have Fort Knox security. The payout for a smaller business might not be as big, but the threat actors can typically find several businesses that might have the same vulnerability and lock all of them down, which makes for a potentially good payday.

Data helps MSPs overcome their clients' misconceptions: 75% of SMBs hit with ransomware would have to shut down as they simply don't have the financial resources to sustain themselves during a security incident. Many SMBs believe an attack will simply take their systems down for a few hours. However, the data shows it is most often days, if not weeks, that their business will be down. We've even seen incidents that last for more than one month—that is a long time to go without a revenue stream and lost productivity. And that's not to mention the costs involved in trying to recover from a security incident, which most likely will include running a PR campaign to restore credibility to your business. All these things can add up and easily approach the 7-figure mark.

Ultimately, the MSPs taking a holistic approach to cybersecurity are the ones that create customer trust. By holistic, we mean looking at the pre-attack phase as well as the post-attack phase. Pre-attack is the tools/technology/compliance part of securing a business as best as possible from a cyber attack, while post-attack is having an adequate cyber insurance policy in place to help make a business whole after an attack.

About the Contributor

Larry Meador

Channel Chief, Datastream Cyber Insurance

Larry Meador is Channel Chief of DataStream Cyber Insurance and is focused on developing and refining partner strategy, deploying partner value programs, and developing industry alliances. Larry has over 20 years of channel experience with businesses such as GreenLink Networks, CNET Content Solutions, Corel Software in addition to having worked in the retail channel for both Circuit City and Computer City in national buying/merchandising. His successes include leading partner acquisition teams, building lasting channel relationships and has won multiple awards as a speaker/presenter at various conferences during his tenure in the channel. Larry is proud of the channel relationships he's built over the years with MSPs and vendors and looks forward to continuing those in this role.

From a personal perspective, Larry is most proud of the three successful young adults he raised as a widower for the past 18 years. He's also an avid bourbon connoisseur as well as an experienced traveler, hiker and photographer and loves to combine all whenever he can!

BeachheadSecure "Checks A Lot of Boxes"

Cam Roberson, VP Sales & Marketing Beachhead Solutions

You might ask: ***"Why this topic?"*** and ***"Why now?"***

The genesis of this Guide began a few weeks ago when I returned from an MSP peer group conference. These shows are always a great opportunity to meet with MSP partners, colleagues, channel friends, and fellow vendors.

I always leverage these opportunities to learn. But there was one subject that just kept bubbling to the top of just about every one of my informal discussions with MSPs: a concern with the ever-increasing visibility of compliance audits, with supply-chain questionnaires, and with what the MSP's role—and opportunity—should be around them. The stakes of not getting this right, with expensive fines, reputational damage and lost business, become more reinforced daily.

I sense that MSPs feel an urgent pressure to understand their compliancy requirements, but are overwhelmed as to how and where to start. MSPs look at the many compliancy rules out there and ask: What really are the differences between these mandates? Do we need to become experts in all of them?

There's a lot to learn about compliancy, and I certainly don't feel at all like an "expert." But my discussions with *real* experts on specific compliancy topics—industry authorities like Paul Redding, Jon DePerro, Larry Meador, Frank Gurnee and Aaron Wyant—gave me the idea to pull their thoughts together as a way to demystify the subject for MSPs and enable them to set smarter priorities. I've known all the experts in this Guide for a long time, and know them (and their firms) to be smart, knowledgeable, and ethical. Their services are top-notch, and I'd recommend any of them without reservation.

My core finding from these conversations is that the different compliancy mandates are far more similar than they are dissimilar. They certainly have different terminology, and different organizational schemes that take getting used to. Some provide general "guidance" for how to comply, while others are extremely specific. One compliancy mandate's gently-phrased call for "data sanitization" is synonymous with another's urgency to "kill" or "blow up" compromised or expired data. Ultimately, every compliancy mandate has the same goal of ensuring data confidentiality and security. That's a good thing, but heck if they aren't nuanced (at best) and downright complicated (at worst) for MSPs, and their clients, to wrap their heads around.

For MSPs, achieving compliancy with relevant frameworks and gaining the ability to tout that compliance with clients is a strong advantage for your practice. Demonstrating your own compliancy and providing the peace of mind that data security is in good hands puts you in position to benefit from more trusting and longer-lasting client relationships, higher MRR, and better margins.

I was thrilled to learn from other vendors—and especially from our security-focused MSP partners—that BeachheadSecure "checks a lot of boxes" for themselves and their clients who are subject to HIPAA, CMMC, FTC Safeguards, ISO 27001, and NIST compliance. Additionally, BeachheadSecure's deep roster of capabilities offers advantageous contributions for improving your and your clients' security profile. Those BeachheadSecure capabilities include: data encryption, MFA & managed authentication, remote access control, geo-tracking and fencing, data sanitization or elimination, behavioral/environmental threat monitoring and automatic mitigation, mobile device/storage protection, enforced authentication policies, logging & reporting, compliance reporting, and more.

We hope this Guide and the expertise herein will help you. Each individual interviewed here has imparted a wealth of valuable information, but they all have much more to share than we could fit into one paper. I would encourage you to consult these experts if their knowledge can be of assistance to you.

Lastly, Beachhead has recently mapped the controls provided by BeachheadSecure to the controls required by CMMC, FTC Safeguards, HIPAA, and the various NIST publications. These findings demonstrate exactly how BeachheadSecure can put you and your clients in a better position to meet compliancy requirements. We invite anyone pursuing compliancy with these controls to review our Compliance Controls Matrix (following pages) to see where BeachheadSecure aligns with your own needs.

Thank you for reading, and we hope you learn something that helps grow and/or strengthen your practice.

Beachhead Solutions Inc.
1150 S. Bascom Avenue
San Jose, CA 95128
Question, comments?
408.496.6936 channelteam@beachheadsolutions.com

BeachheadSecure® Compliance Controls

About this chart:
Chart is organized following the categories delineated in the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover). Identified are the functions provided BeachheadSecure and the controls it satisfies of CMMC Levels 1 & 2, ISO 27001, NIST Cybersecurity Framework and FTC Safeguards.

IDENTIFY

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Asset Management: Inventory of Assets	BeachheadSecure enables remote identification and management of organization's devices		CM.L2-3.4.1	A.8.1.1	ID-AM-1	Section 314(b)
Risk Assessment: Understanding, identifying and documenting cybersecurity risks to organizaiton	BeachheadSecure's RiskResponder meaures, documents and responds to cyberrisks		RA.L2-3.11.1	A.16.1.2,A.16.1.3	ID.RA-1, ID.RA.3, ID.RA.4, ID.RA-5, ID.RA-6	

PROTECT

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Access Controls: Limit and/or protect access to organization's decices and systems	RiskResponder - invalid login attempts	SC.L1-3.1+A15:A233.1+C12:F24	AC.L2-3.1.8	A.9.1.2, A.9.2.3, A.9.2.6, A.9.4.1, A.9.4.2, A.9.4.5, A.12.4.2		
	MFA -Multifactor Authentication	IA.L1-3.5.2	IA.L2-3.5.3		PR.AC-6	Section 314.(c) (1)(i) Section 314.(c) (5)
	Session control	AC.L1-3.1.1	AC.L2-3.1.11			
	Management of access controls (misc)		AC.L2-3.1.12		PR.AC-1, PR.AC-3, PR.C-4, PR.AC-6, PR.AC-7	Section 314.(c) (1)(i)
Data Security: Secure management and protection of organization's data	System- & user-level layered encryption -- protecting data at rest		AC.L2-3.1.19,SC.L2-3.13.11,SC.L2-3.13.16	A.10.1.1, A.10.2, A.14.2.2, A.14.3.1	PR-DS-1	Section 314.(c) (3)
	Data destruction, data quarrantine, data sanitization	MP.2.121	MP.1.118, MP.L1-3.8.3	A.8.3.2, A.11.2.7	PR.D-3	Section 314.(c) (6)(i)
	Protection against data exfiltration (user-level encryption and management of Windows Security Controled Folders)	MP.2.121			PR.DS-5	
	RiskResponder -- protection against data leakage/exfiltraiton through geofencing controls	SC.L1-3.13.1	AC.L2-3.1.19,SC.L2-3.13.11	A.11.1.2,A-12.2.5	PR-DS-4	
	Protection of removable media data, and protecting against unauthorized use of removable media	MP.2.121	MP.L2-3.8.6,MP.L2-3.8.7, MP.L2-3.8.8,AC.L2-3.1.21	A.8.3.1	PR.PT-2	
	protect and encrypt data on mobile devices		AC.L2-3.1.19	A.6.2.1	PR.DS-1	Section 324.(c)(3)
	RiskResponder protects against invalid logon attempts		AC.L2-3.1.8	A.11.1.4	PR.DS-4, PR.DS-5	
Protective Technology -- Technical security solutions are managed to ensure security and resiliance of systems and assets	Audit & logging capabilities	AU.3.045	AU.3.045,AU.L2-3.3.3, IR.3.098, IR.L2-3.6.2	A.12.4.1, A.12.4.3	PR.PT-1	

BeachheadSecure® Compliance Controls

About this chart:
Chart is organized following the categories delineated in the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond and Recover). Identified are the functions provided BeachheadSecure and the controls it satisfies of CMMC Levels 1 & 2, ISO 27001, NIST Cybersecurity Framework and FTC Safeguards.

DETECT

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Asset Management: Secure management of data and stytems	BeachheadSecure multifactor authentication- management of secure access controls	IA.L1-3.5.2	IA.L2-3.5.3	A.9.1.2, A.9.2.3, A.9.2.6, A.9.4.1, A.9.4.2, A.9.4.5, A.12.4.2	DE.AE-1	Section 314(b)
	BeachheadSecure -- analysis and reporting of security events	IA.L1-3.5.2	IR.L2-3.6.2	A.12.4.1	DE.AE-2, DE.AE-3	
Continuous Monitoring: Monitoring for vulnerabalities to systems and data	BeachheadSecure's management of Windows Security and RiskResponder -- continuous monitoring of for potential cybersecurity events and malicious code	SI.L1-3.14.2,SI.L1-3.14.5	RA.L2-3.11.2, SI.L2-3.14.6	A.12.2.1	DE.CM-1, DE-CM-2, DE-CM-3, DE.CM-4	

RESPOND

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Response Procedures and Policies are implemented: Ensuring response to cybersecurity event	Logging and reporting (including Compliancy Report) capability assists in responding to incidents, and facilitates organization awareness of threats	AU.3.045	AU.L2-3.3.3, IR.3.098, IR.L2-3.6.2	A.12.4.1, A.12.4.3,A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.7	RS.RP-1, RS.CO-2, RS.CO-3, RS.CO-5	Section 314(b)
Analysis is Conducted: Ensure effective response and support recovery activities	Logging and reporting (including Compliancy Report) capability assists in the analysis of cyberthreats, and with the implementation of recovery activities	AU.3.045	AU.L2-3.3.3, IR.3.098, IR.L2-3.6.2	A.12.4.1, A.12.4.3,A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.7	RS.AN-1, RS.AN-2, RS.AN-3,RS.AN-4	

RECOVER

Categories	BeachheadSecure Function	Compliance Standard Controls				
		CMMC Level 1	CMMC Level 2	ISO 27001	NIST CSF	FTC Title 16
Recovery processes and planning are improved by incorporating lessons learned	Logging and reporting capability assists identifying vulnerabilites and risks as a part of the recovery process		IR.L2-3.6.1, IR.L2-3.6.2	A.18.2.2	RC.IM-1	Section 314(b)