JARED CASNER & MICHAEL ZBARSKY

FORGING TRUST

MONETIZING COMPLIANCE IN A COMPETITIVE MSP MARKET

Blacksmith InfoSec

Forging Trust

Jared Casner, Michael Zbarsky

Contents

1

Why MSPs Are Ideal Compliance Partners

As you know, managing compliance has become a growing challenge for organizations across industries. With complex regulations like HIPAA, NY DFS, the SEC security rule, and others requiring strict adherence, many businesses are struggling to keep up.

That's why more companies are turning to managed service providers (MSPs) for much-needed help. MSPs offer technical expertise and a deep understanding of compliance requirements, giving businesses the tools and guidance they need to stay compliant while focusing on growth.

Why Are MSPs Considered Go-To Compliance Partners?

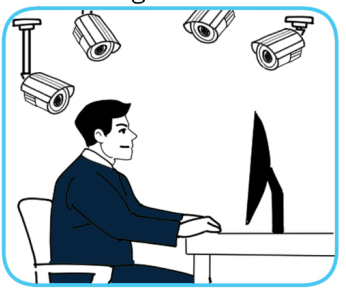
Expertise in technology and security: MSPs stand out as compliance partners due to their specialized knowledge in managing IT systems and protecting sensitive information. With a solid grasp of complex compliance standards, they are crucial for businesses navigating industry regulations.

Ability to offer proactive solutions: The modern MSP doesn't just solve problems as they arise — it prevents them. By offering proactive solutions such as continuous monitoring and vulnerability management, managed IT providers help businesses stay ahead of compliance issues before they become costly problems.

Opportunities for Forging Trust: MSPs are in a unique position to partner with businesses, understand how businesses operate, and become the trusted partner to enhance business processes through technology while providing the cybersecurity needed to keep it all running safely.

Core compliance services MSPs can offer

Monitoring:

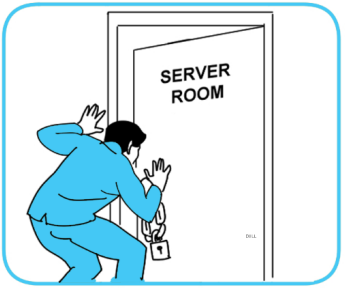


Compliance requires vigilance. MSPs provide monitoring and real-time alerts, as well as detailed reports.

User training:

MSPs deliver targeted training to teach employees how to protect data and adhere to compliance protocols.

Risk assessments:



MSPs identify vulnerabilities within a company's infrastructure, providing clear recommendations to address those risk

Policy development:

MSPs help in creating, implementing, and enforcing these policies to ensure regulatory standards are met.

What Do End-Users Expect from MSPs?

It's not really an option any more; MSPs are expected to play a critical role in helping businesses meet and maintain compliance with industry regulations. Their responsibilities often include:

- **Understanding relevant regulations:** MSPs must stay well-versed in laws and applicable frameworks to advise clients effectively and align their services with compliance requirements.

- **Conducting risk assessments:** MSPs are expected to identify vulnerabilities and risks within a client's IT infrastructure and provide detailed recommendations to mitigate them.

- **Developing and enforcing policies:** MSPs should help create, implement, and enforce comprehensive security policies, enabling their clients to become compliant, more secure, and better align their risk.

- **Offering continuous monitoring:** MSPs are responsible for continuous system monitoring to detect potential threats or non-compliance issues. They are also expected to provide real-time alerts and regular reports to keep businesses informed of their compliance status.

- **Providing user training:** The first line of defense in any organization are the users. Through training the users can form a human firewall to protect the organization. MSPs are expected to educate a client's staff on best practices in data protection and security through tailored training programs.

- **Proactively managing compliance:** Beyond reacting to issues, MSPs should offer proactive solutions like patch management, system updates, and vulnerability assessments to prevent compliance violations before they occur.

- **Documenting compliance efforts:** MSPs must maintain proper documentation of compliance activities, including system audits, incident reports, and risk mitigation efforts, to ensure their clients can provide proof of compliance if audited.

When MSPs Struggle to Monetize Compliance

Many MSPs struggle to monetize compliance services, leading some to opt out of offering compliance at all. If compliance seems too complex or costly to implement, an MSP may decide to press on with a critical gap in their service offerings.

That's exactly why we wrote this book. MSPs can no longer bury their heads in the sand when it comes to compliance — nor should they want to! With the right approach and appropriate tools, your compliance offering can become a reliable source of revenue rather than a source of stress.

2

Identifying the Correct Target Market

When it comes to selling Compliance-as-a-Service, not every business has the same needs or faces the same challenges. MSPs must be strategic in identifying their ideal target market, tailoring their services to address specific industry requirements, and understanding the unique pain points of potential clients. By doing so, MSPs can position themselves as trusted compliance partners, offering the right solutions to the right businesses.

Industry-Specific Compliance Needs

Because different industries are governed by varying regulations, each presents its own set of compliance challenges. To effectively serve clients, MSPs must first understand the specific regulations that apply to each sector. Common regulations MSPs will encounter in the wild include:

- **Healthcare**: With laws like HIPAA, healthcare organizations are required to ensure the confidentiality, integrity, and availability of patient data. MSPs working in this space need to offer services that include encryption, access control, and auditing capabilities, along with risk assessments tailored to protecting sensitive health information.

- **Finance**: The financial sector must adhere to regulations which impose strict data security and reporting requirements like PCI-DSS, SOX, and the SEC Security Rule. MSPs should focus on services such

as secure payment processing, transaction monitoring, and reporting solutions that help financial institutions meet their regulatory obligations.

- **Government**: Government agencies face heightened security and compliance requirements, often dictated by frameworks like NIST and CMMC. MSPs must ensure their services include strong cybersecurity measures, regular audits, and the ability to navigate complex reporting protocols.

By focusing on the specific needs of each industry, MSPs can develop targeted service offerings that address the pain points businesses face in maintaining compliance.

SMBs vs. Large Enterprises and Co-Managed

Company size and structure also play a critical role in determining the compliance needs of a business. Small and medium-sized businesses (SMBs) often lack the internal resources to manage compliance effectively, making them ideal clients for outsourced compliance services. MSPs can provide full-service compliance management, from initial risk assessments to ongoing monitoring and training, giving SMBs the support they need to stay compliant without hiring an in-house team.

On the other hand, **large enterprises** and **co-managed environments** typically have some level of internal IT and security teams in place. Managed service providers can support these organizations by filling in gaps or offering specialized services, such as conducting audits, handling complex reporting, or providing advanced threat detection. The key is to understand how MSPs can complement internal teams rather than replace them, allowing for a seamless partnership.

Tailoring Offerings Based on Company Size and Needs

To maximize effectiveness, MSPs must tailor their offerings based on the size and specific needs of their clients. For example:

- **SMBs**: MSPs may focus on providing all-in-one compliance solutions, handling everything from policy development to training. SMBs often need a more hands-on approach and simplified pricing structures to understand the full value of the service.

- **Enterprises**: Larger organizations might require specialized or advanced services, such as custom policy development, more frequent audits, or detailed reporting that satisfies industry-specific regulators.

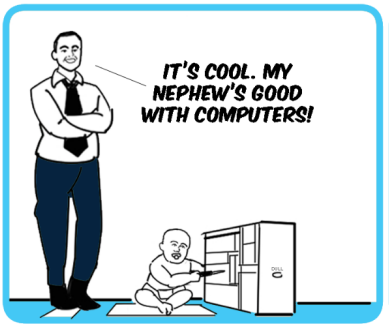
- **Co-Managed Environments**: For clients with existing IT teams, MSPs can offer modular services that align with what the internal team is already managing. For example, an MSP could focus solely on monitoring and reporting while the client's in-house team handles implementation and daily management.

Tailoring services to meet the client's size and unique needs ensures that MSPs remain competitive and relevant, offering value where it's most needed.

Understanding Client Pain Points

Regardless of the industry or size of the business, certain pain points consistently arise when it comes to compliance. MSPs that understand and address these concerns are more likely to build strong relationships and close deals.

Lack of resources:



Many businesses, especially SMBs, lack the manpower or expertise to manage compliance, making it a major burden.

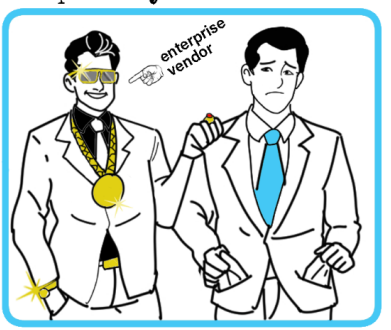
Evolving regulations:

Regulations change frequently, new rules are added, and businesses often struggle to keep up.

Fear of non-compliance:

The risks of non-compliance are high, ranging from fines to legal action or reputational damage.

Complexity and cost:



Businesses want to simplify compliance without spending a fortune.

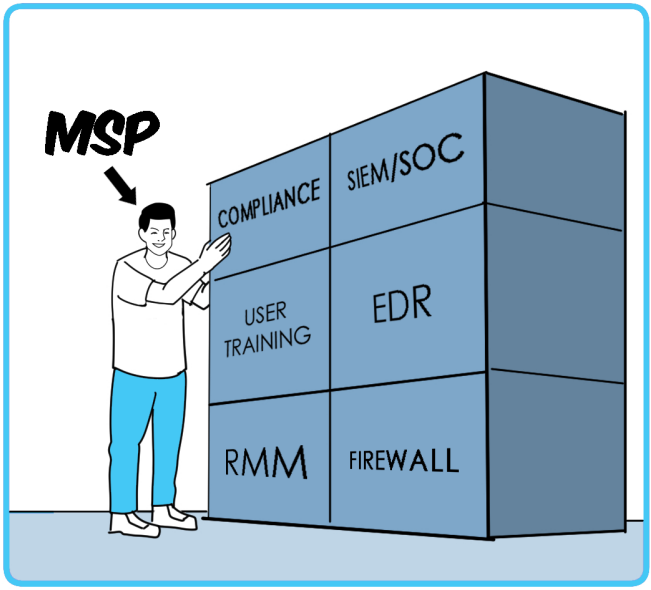
By addressing these pain points directly, MSPs can demonstrate their value, making it easier for potential clients to see the benefits of working together. Blacksmith InfoSec helps MSPs identify these pain points using our built-in Risk Register, and quickly generate Policies that cater to specific needs, ensuring that compliance services are both effective and profitable.

In the next chapter, we'll explore how IT providers can build out their compliance offering, including pricing strategies and Managed Service Agreements.

3

Building a Compliance Offering

Creating a compelling and profitable compliance offering requires careful planning, strategic pricing, and setting clear expectations. Managed service providers need to design packages that meet client needs while ensuring services are delivered effectively and profitably.



Designing Your Compliance Package

The first step in creating a compliance offering is deciding how to present your services. Your package should be designed to attract a wide range of clients while being flexible enough to cater to specific needs. Here are key considerations:

Tiered service models:

A tiered model allows you to offer varying levels of service based on the client's size, industry, or budget. For example, you might have:

- **Basic Compliance**: Entry-level service with minimal features, such as basic risk assessments and policy templates.
- **Advanced Compliance**: Includes continuous monitoring, in-depth risk assessments, and user training.
- **Premium Compliance**: Comprehensive services with detailed reporting, custom policy development, and regular audits.

Tiered models give clients the flexibility to choose a level that fits their needs, and it provides a clear pathway for upselling more advanced services as their compliance needs grow.

Custom vs. standardized packages:

You'll need to decide whether to offer standardized packages that apply to most clients or custom packages tailored to individual business needs. Custom packages provide more value for larger or highly regulated industries, but they can be more resource-intensive to deliver. Standardized packages, on the other hand, are easier to scale and manage but may lack the flexibility needed for certain clients.

Inside and outside an MSA:

The Master Service Agreement or Managed Services Agreement (MSA, either way) is a key contract for MSPs, and deciding whether to bundle compliance into the MSA or offer it as a separate service is critical. Including compliance inside the MSA can streamline billing and reduce the complexity of client agreements. On the other hand, offering compliance as an additional

service outside the MSA allows for more specialized pricing and flexibility in structuring the agreement.

Adding a "compliance" line item to the MSA:

Simply adding compliance as a line item in the MSA makes it easier to introduce CaaS as an integrated part of your offering without overcomplicating your existing contract. By including it as a specific, billable item, clients see the value of compliance as a separate but necessary service, making it easier to justify pricing. Many Blacksmith partners will not take on a client without including compliance in their stack — a choice that most end-users find reasonable as doing so protects all involved parties.

Pricing Strategies

Effective pricing is essential for the success of your compliance offering. You need to balance profitability with competitive pricing that clients will find reasonable. Below are a few pricing strategies that can help:

Value-based pricing:

With value-based pricing, you price your compliance services based on the perceived value to the client rather than the cost of delivering the service. For instance, healthcare providers may be willing to pay more for compliance services because the stakes are higher, while small businesses may require more budget-friendly options. This approach allows you to maximize revenue from high-risk industries while still offering affordable options for SMBs.

Bundling compliance with other MSP services:

Bundling compliance with your other offerings, such as security or network monitoring, can make it easier for clients to adopt. This strategy creates a more comprehensive service package, increasing client retention and satisfaction. Bundling also allows you to cross-sell compliance to clients who may not initially see it as a priority, showing them the value of a well-rounded solution.

Pass-through solution sales:

MSPs can offer compliance tools or third-party solutions as part of their service. Pass-through sales allow you to resell these solutions at a markup, adding

another revenue stream to your compliance package. However, be cautious about how much you rely on this model—clients may expect a significant amount of added value in addition to the software or tools you're selling.

Creating a Service Level Agreement (SLA)

Once your compliance package and pricing strategy are set, you need to define expectations and deliverables clearly. This is where the Service Level Agreement (SLA) comes in. A well-defined SLA sets the boundaries of your service and ensures both you and your client have a mutual understanding of what's included.

Setting expectations:

Your SLA should clearly outline the scope of the compliance services you're providing. This includes:

- The frequency and type of audits or assessments.
- Expected response times for compliance-related incidents.
- How often reports will be generated and delivered.

Defining deliverables:

Make sure you explicitly list what the client will receive, such as:

- Detailed risk assessments.
- Policy creation and updates.
- Continuous monitoring reports.
- User training sessions.

By specifying the deliverables in your SLA, you not only set clear expectations but also protect your MSP from scope creep, ensuring clients understand the full value of your compliance services.

4

Selling Compliance: What MSPs Should Know

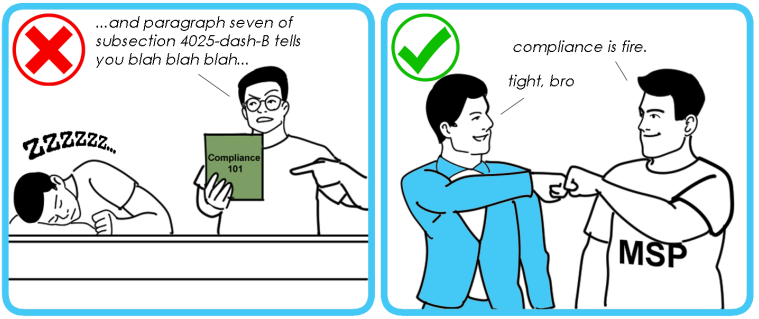
Selling compliance services requires a thoughtful approach that resonates with potential clients, addresses their concerns, and clearly communicates the value of the offering. Many MSPs struggle with finding the "sweet spot" when it comes to positioning, pricing, and selling compliance — often leading to them giving up entirely.

Unfortunately for these providers, the decision to pass on compliance creates its own problems. Not only does it lead to questionable security, but it leaves the MSP at a competitive *dis*advantage. Not to mention missing out on a relatively straightforward stream of revenue.

In this chapter, we will explore effective sales techniques, how to overcome common objections, and the marketing channels that can be leveraged to reach your ideal audience.

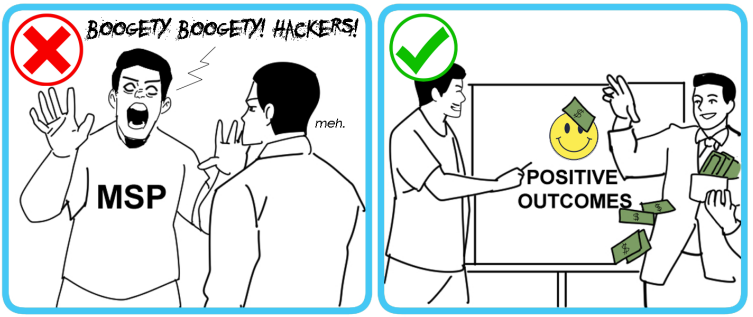
Effective Sales Pitches

Speak on (and in) their terms:



Market wisely:

Don't use fear:



Take a look at these other tips for crafting your sales pitches:

Highlighting the ROI of compliance services in positive terms

Compliance is often seen as a cost center rather than a value-added service. Most MSPs flip the narrative by emphasizing the return on investment (ROI) of staying compliant. By explaining how compliance reduces the risk of costly fines, breaches, or legal issues, they're mostly playing on FUD. As we said, this doesn't always work.

Instead, Give them ideas of how to use this information in their own marketing to bolster their brand — and come ready with case studies of how your other clients leveraged compliance toward greater success, not just avoiding risk.

Agency over policies that you need

Clients want control over their business operations, especially when it comes to policies that affect their day-to-day workflows. Frame your compliance offering as a way to give them agency over their policies. Rather than forcing them to follow a rigid set of guidelines, offer compliance as a tool that empowers them to create custom policies that meet both regulatory standards and their specific business goals. This approach positions your MSP as a partner in their success, rather than just a service provider enforcing rules.

Overcoming Common Objections

In any sales conversation, objections are inevitable. To successfully close deals, it's important to anticipate and address these concerns head-on.

"We don't need it—we're too small to worry about compliance."

Many small businesses assume they aren't large enough to be affected by compliance regulations, or that they can fly under the radar. This is a common misconception. MSPs can counter this objection by explaining that compliance is about protecting the business, no matter the size. Highlight how cyber threats and data breaches don't discriminate based on company size and how non-compliance can result in unexpected costs that could cripple a smaller business. Emphasize that compliance also opens doors to new business opportunities,

especially if they want to work with larger companies or government contracts, which often require strict compliance.

"We already have the policies we need."

Some businesses may feel confident that they already have sufficient compliance policies in place. However, regulations are constantly evolving, and what was compliant last year may no longer meet today's standards. MSPs can handle this objection by offering to review existing policies for gaps or outdated practices. Explain that IT regulatory compliance requires ongoing monitoring, updates, and training to ensure policies remain effective and align with new requirements. Offering a risk assessment as part of your pitch can also demonstrate the value of having an expert review their current framework.

Making Use of the Best Marketing Channels

Beyond one-on-one sales conversations, MSPs can leverage various marketing channels to promote their compliance offerings and reach a broader audience. By targeting the right audience through digital and networking strategies, you can build a steady pipeline of potential clients.

Digital marketing strategies

Online marketing tools like email campaigns, webinars, and social media are cost-effective ways to reach a larger audience. Email campaigns can be tailored to specific industries or business sizes, offering insights on regulatory updates or compliance best practices. Webinars, in particular, are powerful tools for educating potential clients on the importance of compliance while positioning your MSP as a trusted authority. Consider hosting webinars on topics like "How to Prepare for a Compliance Audit" or "Top Compliance Mistakes Small Businesses Make."

Networking and industry events

In-person networking still plays a critical role in building relationships and trust. Attend industry events, conferences, and trade shows where decision-makers in your target industries are likely to gather. These events offer opportunities to meet potential clients, build brand awareness, and demonstrate

your expertise in compliance. Be prepared to offer informational brochures or one-pagers detailing your compliance services and how they can solve common business challenges.

By using both digital and in-person channels, MSPs can ensure they are visible and accessible to businesses that need compliance services, creating multiple touchpoints for engagement.

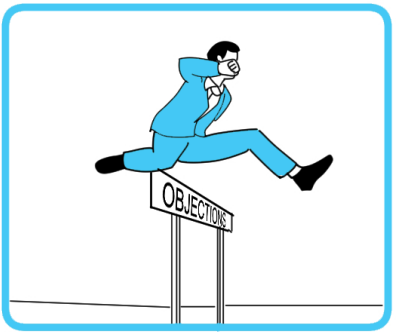
Getting the Sale

Selling compliance services requires more than just a list of offerings—it demands a strategic, client-focused approach. By highlighting the ROI of compliance, speaking directly to the client's needs, and proactively addressing objections, MSPs can effectively convey the value of compliance as a service. Additionally, leveraging digital marketing and networking events will expand your reach and build a stronger client base. With the right sales strategies in place, you'll be well-positioned to grow your compliance offerings and drive long-term business success.

5

Overcoming the Challenges of Selling Compliance

Selling compliance services isn't without its hurdles. Despite the importance of staying compliant with industry regulations, many businesses hesitate to invest in these services. This chapter will explore common hurdles managed service providers face when selling compliance, how to handle objections, and the best ways to prepare your sales team for success.



Common Sales Hurdles

MSPs frequently encounter resistance when pitching compliance services. Understanding the root of these challenges will better equip you to address them.

One of the most common hurdles is reluctance from potential clients, particularly when it comes to investing in something that doesn't directly drive revenue. Compliance often feels like a "nice-to-have" rather than a necessity for many businesses, especially those that haven't faced regulatory scrutiny in the past. For small and medium-sized businesses (SMBs), budget concerns compound this reluctance, as compliance can appear to be an added expense they'd rather avoid.

MSPs typically overcome this by emphasizing the potential risks and costs of non-compliance — with mixed results. While fines, legal fees, and reputational damage from compliance failures far outweigh the cost of proactive management, end users tend to be reductive and dismissive when it comes to these risks.

What's the alternative? Many Blacksmith partners have found success in highlighting the positives around compliance. Rather than hammering clients with FUD (fear, uncertainty, and doubt), they talk about the emotional and practical benefits of being compliant.

Handling Objections

Every sales conversation around compliance will likely involve some degree of pushback. Knowing how to effectively handle these objections will help you turn resistance into opportunity.

"It's too expensive."

Cost is often the first objection raised by potential clients. To counter this, MSPs need to shift the conversation from cost to value. Frame compliance as an investment that protects them from sleepless nights and nagging worry. One strategy is to break down the compliance services into smaller, digestible components, showing how they contribute to the client's overall risk mitiga-

tion strategy. You can also take the approach of including compliance in your cybersecurity stack rather than treating it as an *à la carte* item. (It's quite easy to show the value and importance of it when you make it clear that you simply won't take on a client who doesn't maintain compliance.)

"We've never had an issue, so why invest now?"

Clients who have never experienced a compliance breach or audit may feel they don't need to invest in compliance services. This objection can be tackled by explaining that compliance is about future-proofing their business. Regulatory requirements are constantly evolving, and being reactive rather than proactive can lead to expensive, last-minute fixes. Present compliance as a preventative measure that ensures their business is ready for any regulatory audits or changes. A good analogy to use relates compliance to a 401(k) plan: If you wait until you're close to retirement to invest in your 401(k), you'll need to invest a ton of cash to fill the account. However, if you start investing early, even small amounts of early capital will accrue into a much larger value.

"We already have someone handling compliance."

If a client claims to have compliance covered in-house or through another provider, it's important to differentiate your MSP's services. Ask detailed questions about how they are currently managing compliance and whether their internal team has the expertise to stay up-to-date with changing regulations. Offer a complimentary risk assessment to highlight any gaps or areas of improvement. This approach not only demonstrates your value but also positions you as a proactive partner rather than a replacement.

Training Your Sales Team

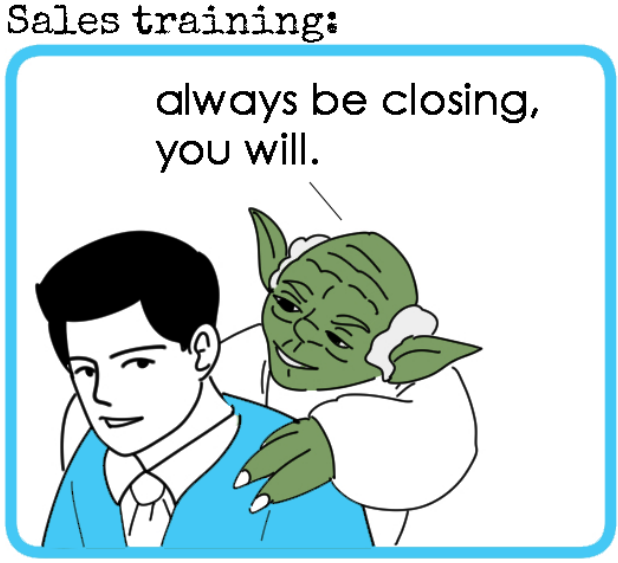
Selling compliance is complex, and your sales team needs to be well-equipped to handle the intricacies of this service. Proper training is key to ensuring they can communicate the value of compliance and handle objections confidently.

Understanding the value and intricacies of compliance services

Your sales team should have a deep understanding of both the technical and

regulatory aspects of compliance. They need to be able to explain how your MSP's services align with specific industry regulations, whether it's HIPAA for healthcare or PCI-DSS for finance. This level of expertise builds credibility and helps the sales team effectively articulate the importance of compliance to potential clients.

Regular training sessions can keep the team up to date with the latest regulatory changes and help them refine their sales pitch. You may also consider role-playing exercises where team members practice handling objections or explaining compliance services to different types of clients, from SMBs to large enterprises.



Focusing on consultative selling

Compliance isn't a one-size-fits-all solution, and your sales team should adopt a consultative approach. Encourage them to listen carefully to the client's specific needs and pain points, and use a compliance tool or software solution that both works with all clients **and** allows you to custom-tailor their experience.

Providing sales collateral and resources

Equip your team with case studies, whitepapers, and brochures that demon-

strate the success of your compliance services. These resources provide tangible proof of your MSP's ability to deliver results and help your sales team build trust with potential clients. Additionally, offering demos or free assessments can lower the barrier to entry for prospects, making it easier for them to see the value of compliance before committing. Using a compliance solution like Blacksmith gives you even more opportunities, such as free trial periods wherein your client can experience policy management firsthand.

6

Supporting and Growing Compliance Services

Delivering compliance services doesn't end with the initial sale. For long-term success, managed service providers (MSPs) must focus on onboarding clients efficiently, scaling their services, and maintaining continuous engagement. Today, we'll explore strategies for ensuring smooth client onboarding, implementing scalable solutions, and driving additional revenue through ongoing engagement and upselling.

Onboarding New Clients

The first step in delivering compliance services is onboarding new clients in a way that sets the stage for a successful partnership. A structured onboarding process not only helps build trust but also ensures that your compliance services are aligned with the client's specific needs from the outset.

Best practices for a smooth transition:

A smooth, painless onboarding process is essential for ensuring clients understand their compliance requirements and the role your MSP will play in meeting them. Start with a comprehensive risk assessment to identify potential vulnerabilities and gaps in their current compliance posture. This allows you to prioritize issues based on risk level and regulatory urgency. Ensure you're communicating clearly with the client throughout, explaining what each step entails and how it contributes to their overall compliance.

Blacksmith InfoSec onboarding approach:

Blacksmith InfoSec emphasizes the importance of a holistic security program and smooth onboarding. By aligning policy creation to frameworks, MSPs can streamline compliance with a fully-aligned roadmap. This plan prioritizes a list of actions, beginning with the most critical risks, turning compliance into a set of manageable tasks. The result is an approach that helps the client feel more in control of the process while providing a structured plan for success.

Policies and risk factor priority:

A key part of onboarding involves creating or updating the client's compliance policies. Typically, businesses will need policies covering areas like data security, access control, and incident response. Policies can be deployed as a single long, all encompassing, information security policy or as numerous policies covering the information security program. Policies are the infrastructure that the security program will be based on and should be deployed to provide the roadmap to compliance.

Scaling a solution that stays profitable:

As your client base grows, your compliance services need to scale without

increasing costs disproportionately. This means standardizing processes where possible, automating routine tasks like monitoring and reporting, and offering tiered service levels to accommodate different client needs. Blacksmith InfoSec provides tools that allow MSPs to scale their compliance services while keeping them profitable, such as automating policy updates and enabling risk management, ensuring that even as your client roster grows, your services remain efficient and scalable.

Continuous Client Engagement

Once onboarding is complete, the next challenge is maintaining regular engagement with clients. Continuous communication not only ensures compliance standards are met but also provides opportunities to upsell additional services.

Regular check-ins and updates:

Regular communication is key to keeping clients informed and engaged with their compliance efforts. Schedule periodic check-ins—whether monthly or quarterly—where you provide clients with compliance reports, updates on regulatory changes, and any recommendations for policy adjustments. This proactive approach helps clients stay on top of their compliance obligations and builds trust in your MSP as a long-term partner.

Upselling additional services:

Continuous engagement also opens the door for upselling. As clients become more comfortable with basic compliance services, they may need additional offerings such as advanced threat detection, custom policy development, or specialized audits. Take advantage of regular client meetings to identify new pain points and offer cybersecurity solutions that align with their evolving needs. For example, if a client's business is expanding into a new market or industry, they may need additional compliance support to meet new regulatory demands.

Upselling can also include bundling compliance with other services you already offer, such as managed security, disaster recovery, or SIEM/SOC. By integrating compliance with these services, you provide clients with a more

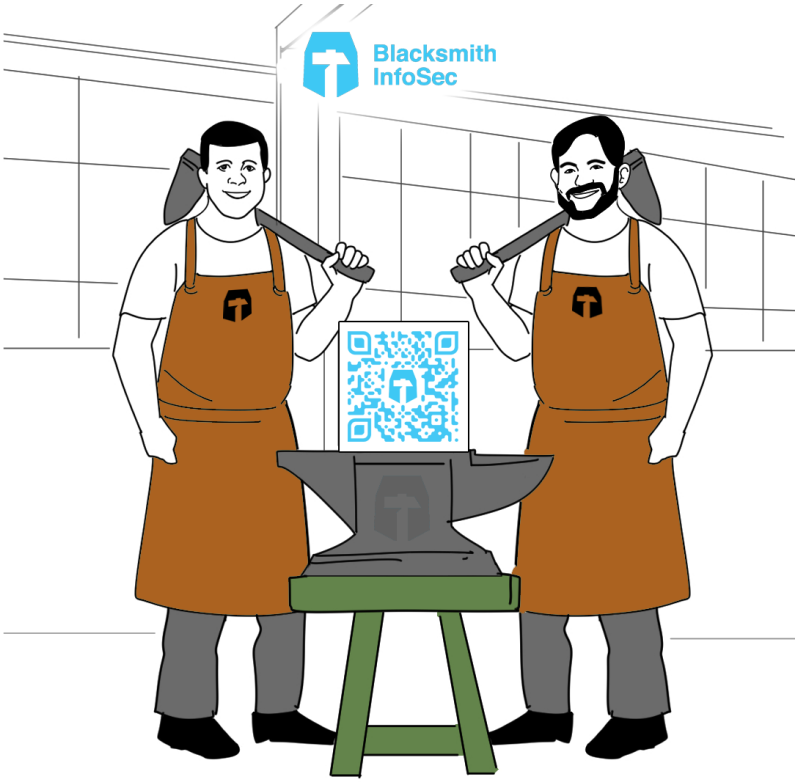
comprehensive solution, increasing their reliance on your MSP and driving additional revenue.

Forging Ahead

Supporting and growing your compliance services requires a strategic focus on client onboarding, scalable solutions, and ongoing engagement. By following best practices for onboarding new clients, ensuring your solutions can scale profitably, and maintaining continuous communication, you can not only meet client needs but also create opportunities for upselling and expanding your service offerings.

Thanks for Reading!

We hope you enjoyed learning more about Forging Trust with your clients. To see Blacksmith in action, scan the QR code below to schedule a demo!



FORGE TRUST WITH YOUR MSP CLIENTS THROUGH PROFITABLE COMPLIANCE SERVICES.