

Top 3 Things to Know About Security Frameworks

Want to build a security practice but not sure where to get started? Start with the topic of Security Frameworks! Frameworks are designed to help organizations get a footing in security and provide a focus for elements to be covered within your business. We spoke with Jacob White, Cybersecurity Technology Consultant II, to learn more.

#1 - Security frameworks help you develop a starting point.

Many organizations don't know how to get started with building a security practice, but frameworks are here to help guide the process. Starting with a framework will provide a roadmap or guiding light of the most important bases to cover, security concerns to address, controls to implement, and recurring opportunities to manage with your customer base. A framework will guide technology resellers on the best areas to sell into, what products to offer, and what services to champion. Standardizing to a security framework also helps introduce customers into the security sales cycle, a continuous process of selling, and evaluation, and re-evaluation of the environment.

#2 – There are various frameworks to choose from that meet your needs.

There are different frameworks, from the NIST CSF that Ingram Micro uses to frame up its Security Sales Cycle, to CIS Top 20, COBIT, MITRE, and others. There's no wrong answer on which one you pick, so don't get caught up in worrying about which is right - it's all about what is the best fit for your company and culture. NIST is a great overall framework to start with as it's very comprehensive with different levels varying from basic to more granular. The Center for Internet Security (CIS) Top 20 Security Controls is simplified and a great starter framework, and MITRE is advanced, very granular, and focused on what attackers are doing. Get started by digging in and reading the available frameworks, picking one that's right for you, and then building a plan to implement.

#3 - Ask for help from industry experts and consultants.

Getting started with a framework can result in an overload of information, but Ingram Micro's consultant experts like the Cybersecurity Delta Force are here to help demystify the process. You don't have to do it alone – using peer networks like Ingram Micro's SMB Alliance and Trust X alliance can offer valuable feedback and support from folks who have been there already.

Learn more about each of the foremost frameworks:

[Cybersecurity Framework | NIST](#)

[The 20 CIS Controls & Resources | Center for Internet Security](#)

[COBIT | ISACA](#)

Ingram Micro's Cybersecurity Delta Force is here to help you determine what's best for the environment in question. Leverage our team to help work through available options that meet your needs and maximize security posture. Contact us at cybersecurity@ingrammicro.com to learn more!