GreyCastle security

PRODUCT STORY SERIES:

Earning more RFP wins with Policy Framework and Policy Development

This engineering firm took their cybersecurity documentation from zero to sixty — now they can win more contracts!

Today, the savvy customer is evaluating everything about their potential vendors, including their cybersecurity programs. They're asking more and more frequently, "How is this contractor going to handle my information?" Documentation is a straightforward way to demonstrate the strength of your cybersecurity program to prospects (on top of supporting your security program), but creating it can be tedious and time-consuming. Follow the lead of this GreyCastle Security client and let an expert handle it for you so that you can focus on your core business offerings.

Client At-A-Glance:

Industry: Civil Engineering & Architecture
Employees: 1000+
Revenue: $100 to $500 million
Goal: CMMC Certification

Jared* is the Chief Information Officer of a large civil engineering firm. They've planned and executed high-profile infrastructure and architecture projects throughout North America, and they know they can do even more. Executive leadership wants to work on more sensitive government projects, but to even bid on those RFPs, they will need government cybersecurity certifications like CMMC or DFARS. Jared is told that since his department manages IT, his department should be able to get the company compliant with the relevant laws.

While the firm itself is sizable, it's also very decentralized, and 'corporate' teams like IT don't have as many people or resources as a company this size might typically demand. Jared and his team have been busy keeping the engineers and project managers working; they haven't had the bandwidth to formalize a cybersecurity program — where would they find the time? Jared and his team know enough to keep their own data safe, but they lacked the expertise to manage the security of the whole firm. They weren't confident they could create and implement a program robust enough to meet government compliance regulations.

*Real names omitted

After bringing GreyCastle Security on for a Risk Assessment, Jared decided to purchase our ***Policy Framework*** service. GreyCastle Security performed an intensive two-day workshop, interviewing department leaders across the organization. Our team of security experts determined the firm's risk, business, and compliance needs and created a massive library of client-branded cybersecurity documents ready for implementation. Jared now had a documented Information Security Policy, a Business Continuity Plan, an Access Management Procedure, and much more. The framework documents established cybersecurity ownership and responsibilities across departments, including a Cybersecurity Steering Committee to manage the program going forward.

"The structure of the biweekly meetings and the efficiency of the GCS policy library helped Jared solve his very real, complex issue."

After establishing a baseline and understanding the full scope of a comprehensive cybersecurity program, Jared saw the value in having a long-term security partner. He brought GreyCastle Security on for ***Policy Development*** services. We scheduled biweekly meetings with Jared and his team to adjust and finesse their new policies based on specific implementation challenges they encountered. He has regular access to a pool of security experts who can custom tailor policy solutions for the firm.

With the Policy Framework, Jared got the documentation he needed to get certified and bid on contracts. With Policy Development, he strengthened his cybersecurity program to an auditable position that can win RFPs. While the CMMC framework has been delayed, our client is set to handily pass their upcoming DFARS audit and is ready for certification. Jared repeatedly tells us in meetings how happy he is to have a long-term cybersecurity partner, and he's brought GreyCastle Security in as a virtual Chief Information Security Officer for the firm.

Jared is not the first CIO to find himself suddenly in need of documentation — we see this issue with many clients across industries. It takes time to create and doesn't feel like it's directly contributing to your business goals. However, a well-documented set of policies, procedures, and standards can align your organization and create value for you and your clients. If you don't have the resources to create documentation from scratch, bringing in a cybersecurity partner may be the most efficient solution.

For more information, see:

- **Infographic: 3 Ways to Align Cybersecurity with Business Goals**
- **Podcast: Compliant Doesn't Always Mean Secure**
- **Podcast: Where to Begin with CMMC Compliance**

Reach out to an advisor for a consultation about your policy needs:

Contact Us:

greycastlesecurity.com
/company/greycastlesec
@greycastlesec
intel@greycastlesecurity.com
(800) 403-8350