



CASE STUDY: Manufacturing company faces challenge of meeting compliance of NIST 800-171 to maintain status as subcontractor.

BACKGROUND

A manufacturing company was at risk of losing their status as a subcontractor for contracts that include Controlled Unclassified Information (CUI).

Cybersecurity had not been a priority for them in the past, and an initial gap assessment performed by a local consultant had left them with a stack of paper full of red to show the controls that they were not currently meeting, but no real guidance on how to get from their current state to a compliant one. This was becoming critical as failure to meet the requirements by December 2017 would result in the company no longer being eligible to receive contracts that are worth hundreds of thousands of dollars in revenue to the business.

OBJECTIVES

- Identify where Controlled Unclassified Information (CUI) is transmitted or stored
- Verify gaps in compliance for NIST 800-171
- Confirm if other compliance(s) may also apply, such as HIPAA or PCI
- Provide detailed recommendations for remediation

SOLUTION

The first step was to take the gap assessment report that they had already paid for and turn it into meaningful and useful information for them. We did this by assigning a NIST auditor to validate the findings with their internal IT team. We found that while most were correct, in some cases were they had been marked as “not compliant” a control was actually in place that met the requirement, in other cases where they were shown as “compliant”, there was not actually a solution that met the standard. This is something we see often when other consultants rely too heavily on a client’s responses to a compliance questionnaire and do not perform their own validation or do not have the technical background to understand the controls.

Foresite’s auditor was also able to look at the types of data being transmitted and stored by the company to explain where other compliances, such as HIPAA and PCI would apply. Fortunately many of the other compliances are based on the NIST standard, so the control requirements overlap and can be met by a single solution.

The next step was to take the findings and turn them into targeted recommendations that met both the NIST 800-171 requirement and the business needs. There is usually more than one way to meet a control, so the needs, culture and budget of the business should be taken into consideration when making recommendations. Foresite’s auditor sat down with IT, the business owner, and other key staff from each department as part of this process.

Finally, we reviewed the recommendations with the business owner and his team. While they were comfortable that they could handle many of the required steps on their own, they asked for quotes on some hardware and software solutions from our Channel Partner, and also asked to engage Foresite on an ongoing consulting basis to assist them as they put together some of the missing documentation and processes so we can confirm that the results meet the NIST 800-171 standard. They feel confident that they are on the right path now, and will not have any problem meeting the deadline for compliance.

INDUSTRY

Manufacturing

BUSINESS CHALLENGES

- Requirement to meet compliance by deadline or lose hundreds of thousands of dollars’ worth of contracts
- Outside consultant provided assessment that didn’t provide a road map to compliance
- Internal staff did not know what needed to be done, or how to do it.

FORESITE SOLUTION

- NIST 800-171 Advisory Consulting

OPPORTUNITIES

- Leverage the previous consultant’s report to make use of that investment
- Obtain detailed “road map” to compliance and an ongoing consulting relationship to meet the

deadline and maintain the revenue.