

# COMPLIANCE WEEK

THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

## Case Study: Alaskan Utility Gets SOX Compliant

### COMPANY BASICS

Company Chugach Electric Association Headquarters Anchorage, Alaska Employees 330  
Industry Utilities Revenue \$288 million

### THE CHALLENGE

Chugach faced two areas of concern in maintaining Sarbanes-Oxley compliance: its massive construction and maintenance costs, and the fact that its position as an electrical co-op both generating and distributing power made it an extreme rarity, with no case examples existing for how to comply with SOX.

### SOLUTION CHOSEN

Step one was to manually process documents with help from Certified Security Solutions; second, identify what transactions KPMG would want to test; third, define key controls; and, last, sign up for Brainloop Secure Dataroom for assistance with control key spreadsheets, and Tripwire for system configuration control and change assessment.

By Todd Neff — November 10, 2009

This “case study” is the latest in a series of articles aimed at helping public companies understand how other organizations are using technology to comply with new regulations and standards. These are **not** advertisements or marketing vehicles for the companies mentioned; Compliance Week’s editorial staff speaks with the public company that has deployed the technology, and the article is written without the input—and in many cases the knowledge—of the vendor.

Doing business as an electric utility in Alaska has its special challenges, such as bad weather and sometimes uncertain fuel supplies. But as the leaders of Chugach Electric Association, Alaska’s largest electric utility, will tell you, regulatory compliance is much the same there as in the Lower 48.

Chugach (pronounced *chew-gatch*), based in Anchorage with \$288 million and 330 employees, provides electricity to 70,000 retail customers in and around Alaska’s largest city. It also sells wholesale energy to smaller utilities stretching around the “Rail Belt” connecting Homer, Anchorage, Fairbanks, and points between.

Technically the business is a cooperative, owned by its members rather than stockholders of the sort that Sarbanes-Oxley Act aims to protect. But Chugach issued publicly traded bonds in the 1990s that first brought it under the purview of the Securities and Exchange

Commission, and in 2007 its outside auditor KPMG delivered another dose of reality: The utility had to submit to SOX compliance as a small filer.



Dave Smith, senior vice president of administration for Chugach, knew Sarbanes compliance wouldn't be an easy feat, especially with the unique challenges Chugach faces. One wrinkle, for example, was the massive construction and maintenance cost associated with the utility's generation and transmission infrastructure. Another, Smith says, was Chugach's unusual situation of both providing and distributing power—making the company “kind of an island” when it comes to complying with Sarbanes-Oxley.

And then there was the small question of how to pay for all that compliance. “We watched all the large filers spend millions of dollars trying to become Sarbanes-Oxley compliant,” Smith says. “We couldn't afford that.”

So, Smith took actions that he knew the company could afford.

The company knew it would need some help, Smith says, and turned to Certified Security Solutions, a consulting firm based in Portland, Oreg. About 20 Chugach employees did most of the process documentation, with the consultant focusing on strategy and program management.

“The only full-time people were the two people from the consulting firm who provided oversight, guidance, and the kick in the butt we needed,” Smith said.

The first step was to identify the transactions KPMG would want to test, which were then classified into nine “cycles.” Those cycles included revenue, supply chain, payroll, financial reporting, treasury, and cash management, among others.

Once those processes were identified, the definition of key controls could begin. Like many companies circa 2007, says Cheryl Klein, the certified security consultant who worked with Chugach, the business had too many of them.

“A lot of times organizations still have too many key controls,” says Klein (who has since set up her own shop as GRC Consulting Services). “It's not to say [all controls] are *not* important—or that Sally or Joe or whoever performs them aren't important. It's that for enterprise risk and compliance, we don't have to, as auditors, test them.”

Remember that Chugach began its effort in 2007, when companies and their audit firms still labored under the exacting language of Auditing Standard No. 2 from the Public Company Accounting Oversight Board. Total number of key controls Chugach tallied up that first year: 230. Ouch.

“It was like going to the doctor and they say you need 10 tests,” Smith says.

By 2008, however, the fog around SOX compliance had lifted. The PCAOB scrapped AS2 in favor of the much more relaxed Auditing Standard No. 5. That allowed Chugach to reduce its key controls by about two-thirds, Smith says.

### **Getting Automated**

As the project unfolded, Klein pushed for control automation as much as possible, arguing that automation pays for itself in reduced compliance and audit expenses down the road. She suggested Chugach first take full advantage of the software it had already purchased.

At the time, Chugach was in the midst of implementing Oracle's PeopleSoft modules for financial, HR, and payroll functions—which offer “a lot of financial controls that organizations don't recognize or take advantage of,” Klein says. Examples include automating checks for duplicate invoices and performing three-way matches of invoices, purchase orders, and receiving confirmations.

“Sometimes organizations don't have it set up in their systems; other times, they have it set up but don't have it identified as a control they can rely on,” Klein explains.

Many of Chugach's key controls required keeping track of spreadsheets. A single monthly journal entry to post depreciation to Chugach's many assets stemmed from more than 30 different spreadsheets. Revenue from wholesale electricity sales—millions of dollars a month—was tracked via spreadsheets being e-mailed around.

“You've got a general ledger accountant that's been here 18 years and a rates person who's been here 23 years and you know they're honest, but we were dealing with \$14 to \$15 million bills with no control every month,” Smith says. “I don't want to say we were crazy, but that was the case.”



Here, Chugach's SOX compliance effort fell into step with its ongoing work to improve IT security and compliance practices. Although Chugach outsourced credit card processing, the company was familiar with PCI compliance standards and had increasingly used ITIL (Information Technology Infrastructure Library) as an IT management framework, says Dwight Dial, Chugach's director of information services.

“It's doing things that we needed to do anyway for security reasons, so we had all the activities going on that compliance requires,” Dial says. “We just didn't necessarily have it all documented or all the evidence required by an auditor.”

The SOX effort brought new software tools in two areas. First, to control key spreadsheets, Chugach signed up for Brainloop Secure Dataroom, a secure hosted service that allows collaboration while restricting access to critical spreadsheets and providing an exhaustive audit trail of changes to them. Chugach spreadsheets relevant to the financial-reporting process all live in the Dataroom now, Dial says.

Brainloop allows for “very granular management of all the documents you house, so you know who changed what and what they changed, and you can lock down files that can’t be changed,” Smith says.

Second, for detective controls on systems hosting anything requiring SOX compliance, Chugach added Tripwire for system configuration control and change assessment.

The SEC has pushed back the SOX compliance deadline for small companies like Chugach into 2010, but the company is already on its second SOX audit with KPMG. The combination of automation and manual testing will cost \$70,000 to \$90,000 a year in internal man-hours, Smith says. Many of the processes remain manual.

On the IT side alone, Dial says, “We’ve added a full-time equivalent’s worth of work, and nobody to do it. It changes our priorities, but that’s alright. You have to be used to change, you know.”

---

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.