

Genzyme Corporation

SMP's singular focus is

IT security audit and assessment professional services. Our vendor-neutral, in-depth IT Assurance consulting approach leverages best practice and compliance expertise from hundreds of engagements. SMP will reduce your company's vulnerabilities, brace operational and network infrastructure security, and facilitate compliance with evolving government regulations. We provide concrete, actionable recommendations to help you identify, achieve, and maintain the right level of security.

Industry: Biotechnology

Company Bio: Founded in 1981, Genzyme is one of the world's leading biotechnology companies dedicated to improving the lives of people with debilitating illnesses. As a Sanofi company with 2010 revenues in excess of \$4.05 billion, Genzyme's technologies, products, and services help patients in approximately 100 countries worldwide and focus on many areas including cancer, kidney disease, rare inherited disorders, transplant and immune disease, and diagnostic testing.

World Headquarters: Cambridge, Massachusetts

Employees and Locations: 10,000 employees in 40 countries spanning the globe across 65 company locations including Africa, Europe, the Americas, and the Middle East.

“SMP'S REGULATORY EXPERTISE

was essential in enabling our efforts to impart the importance of understanding and following the new MA security regulations. They created and conducted a very powerful internal webinar that really hit home with our data stewards. We have used SMP for multiple projects including technical audit services, regulatory compliance reviews, and security consulting engagements. They have exceeded our expectations every time.”

— **BOB LITTERER**
Sr. Director, Information Security
Genzyme Corporation

Objective

Genzyme engaged Security Management Partners (SMP) to guide their compliance effort with Massachusetts 201 CMR 17.00. This regulation establishes minimum standards to safeguard personal information about a MA resident, in paper or electronic form, held by businesses who own, license, store or maintain that data. It requires: 1) training for individuals responsible for ongoing data management; 2) a written information security program consistent with industry standards; 3) a series of administrative, technical, and physical safeguards, including encryption, user authentication and access restrictions; 4) thorough interview, observation and policy review; and 5) remediation recourse if necessary.

Process

First, SMP conducted a live online meeting with the Genzyme employees responsible for handling company data to discuss the content and ramifications of MA 201 CMR 17.00 to the Corporation. Next, SMP created a customized survey to obtain information about the company's data collection and storage procedures. Then, SMP conducted a statistical gap analysis based on the results of the survey to determine if holes exist. Finally, Genzyme was provided with a documented analysis and commentary on any policies already in place and the requirement for new policies to govern data.