ISO 27001 COMPLIANCE

Walter B. Riddock, CMDSM, M-EDP, EMCM
Chief Executive Officer
Direct Mail Systems, Inc.

One of our major clients, as part of doing business with them, required us to become ISO 27001 certified, and insure that we are compliant with applicable Medicare regulatory program requirements, as well as CMS rules and guidance including HIPAA Privacy.

We recognized that we had a lot to do but did not know where to start. We knew that our company had well-established policies and processes to monitor and manage customer and financial data, operational and communications infrastructure, software, internal and externally-facing websites. Still, we felt that there was room for improvement, yet we did not know what we needed to do and how much needed to be done.

After interviewing five companies we selected Security Compliance Associates (SCA) to perform our information security assessment and provide us with a Gap Analysis. We believed their fees for the proposed services were reasonable and that we could accomplish attaining ISO 27001 compliance without the big cost others were presenting. Boy was I right.

Security Compliance Associates *performed an expert examination that* provided an extensive Information Technology Vulnerability and Cybersecurity Assessment, as well as a review of our physical security of the business's information systems and our facility.

Their Security Review & Gap Analysis provided us with a complete process for defining security risk strategies based upon our objectives and the potential impact to our business. Their audit showed us exactly what people, processes and technologies were most at risk so that we could focus our efforts on addressing the issues that matter the most.

Their Cyber Security tests diagnosed actual vulnerabilities associated with penetration testing, vulnerability testing and phishing tests, along with external networks, Websites, Web applications as well as internal networks.

SCA provided a custom report that offered specific vulnerability findings, prioritization, recommendations and remediation advice.

After we implemented new processes and procedures, made extensive changes to our IT infrastructure and modifications to our facility, we became ISO27001 compliant.

In summary, we have built a lifetime partnership with SCA.