

## AuditOne Advisory

From Bud Genovese, CEO

### Time for a Technology Tune-Up?

We're hearing from the field that regulatory examiners are paying close attention to the security of bank IT networks and systems. As you know, regulators now emphasize a risk-based approach to IT examinations, and IT examinations are now specialty exams conducted annually by the FDIC and other regulators. Banks must develop a coordinated risk management program that highlights the relationship between business-related risk management and technology-related risk management. Today's prudent technology risk management program should include an annual IT risk assessment, an information security review, an independent IT audit, review of bank-wide business continuity plans, network penetration tests with social engineering analysis, and a review of the Information Security Program (federal GLBA and applicable state laws).

Because technology marches swiftly forward (hopefully with hackers at least several steps behind), industry experts now recommend that banks perform IT audits on an annual basis. This schedule is prudent in part due to the advance of new productivity-enhancing technology being deployed across the corporate landscape. For example, many institutions are considering or already have introduced iPhones for their employees, but it's critical to manage the special encryption limitations that exist for iPhone data in-transit and at-rest. Remote deposit capture is still relatively new, and it's important to examine its risks. And the latest regulatory hot-button issue is pandemics. Is your bank's Business Continuity Plan up to date to deal with this issue? Perhaps it's time to consider a technology tune-up for your bank.

AuditOne's team of highly certified technology experts hold CISSP certifications, the highest technical standard in the information security industry, and have had real world experience operational experience inside billion-dollar financial institutions. Our IT audits are based upon the latest FFIEC Information Security Exam Guidelines and other standards recommended within those guidelines such ISO17799-2005.

And our technology experts go the extra mile for you by taking a consultative approach toward the audits. Because we have more than 150 clients, we have a good idea of what works and what doesn't (although we cannot recommend specific vendors or products). We offer insightful, practical recommendations and counsel on how to resolve each finding.

AuditOne's full range of deep technology services include Information Technology (IT) Audits, Electronic Banking (with Cash Management, Remote Capture) Audits, External and Internal Network Penetration Testing with Social Engineering Analysis, and consulting for specific aspects of Information Security Risk Assessment (methodologies), Business Continuity Planning (Business Impact Assessments), and other Information Security policies and procedures.

Knowing that technology is constantly changing and that regulators are likely to look deep inside your bank's technology engine, the safe and sound approach is to call AuditOne for the most thorough and up-to-date technology tune-up in the internal auditing industry.

*Bud Genovese is founder and CEO of AuditOne LLC, a San Jose, California-based internal audit firm that focuses only on banks and their service providers. Mr. Genovese pioneered the concept of providing comprehensive, affordable, independent internal audit services by gathering wide-ranging, world-class expertise within one firm. AuditOne serves over 90 clients throughout California, the Western United States, and nationally.*

Contact Bud Genovese at 408-980-8099 or [bud.genovese@audit-one.com](mailto:bud.genovese@audit-one.com); Website: [www.audit-one.com](http://www.audit-one.com)