TBS Technology & Business Solutions
It's time to expect more

COMPLIANCE IN THE CLOUD. MORE THAN HOT AIR.

In this whitepaper, Technology & Business Solutions LLC co-founders Jay Ethridge and Joe Jezior demystify the alphabet soup of regulatory acronyms that govern accounting system compliance in The Cloud – SSAE16, ITAR, MA201, SOX, CMS, DISA, etc. The bottom line? When it comes to Deltek Cloud Hosting, not all compliance environments are the same, and a "SAS 70 Type II facility" typically only means that the provider locks its server room doors at night. Of course, safeguarding and securing your most important and sensitive financial data requires much, much more than that.

At Technology & Business Solutions we're proud of our role in helping our customers attain the most secure, flexible and scalable technology framework for the financial management of their organizations. Our clients have entrusted us with a solemn responsibility – to ensure that their financial data is safe, that it's disaster-proof and that it's always available. Hand and hand with that mission, TBS delivers the most regulatory compliant environment for Deltek and QuickBooks data and applications.

We've also found that throughout our almost ten years in business as Deltek's first and largest cloud hosting provider, achieving a fully compliant Deltek accounting system is a topic that bears some explaining. It's not as simple as it sounds.

Any business that has contracts with a federal agency or department at some point is subject to several important regulatory regimes that monitor and control their financial data and accounting systems. Here's a brief overview of the four most important.

A. The GSA or DCAA Financial Audit. Though audit thresholds vary, in general all government contractors at a minimum defined size must submit an annual Financial Audit Report to the appropriate procurement agency. Smaller enterprises that are growing rapidly, plan to sell, or partner with larger organizations on contract bidding and services also often fall under such requirements. And, of course, making sure that your financial system meets the published security standards for government contract accounting is just good business, audit or not.

Under GSA or DCAA rules your business must ensure it maintains "full system control" over its accounting IT infrastructure. This means designated-employee-only access to your accounting hardware and IT facilities, your server operating systems, your databases, and your Deltek software too. (You need all four control facets to fully comply.) It's important to note that if you host your Deltek system with a third party, a "SAS 70 Type II facility" on its own DOES NOT meet this full system control standard. Frankly, commodity data storage farms like Rackspace and Amazon boast SAS 70 facilities, but a facilities designation does NOT cover your data, system access, or applications.

B. ITAR. The International Traffic in Arms Regulations apply the important mandates of the Arms Export Control Act to any business engaged in the "export and import of defense articles and services." ITAR is administered and audited by the U.S. Department of State, and includes sweeping standards for the handling and security of accounting and financial data. Two fundamental ITAR requirements are that only U.S. citizens may access your accounting IT infrastructure, and that all financial data and applications must be physically located in the continental United States – this includes any hosted accounting data or accounting software too. **At TBS, our hosting platform and hosting centers are fully ITAR compliant. We're the only Deltek Enterprise Cloud that is.**

C. MA201. From a personnel privacy perspective, the recent MA201 "Standards for the Protection of Personal Information" cover any business with employees or subcontractors that are residents of Massachusetts. *At least seven other states are actively considering legislation that will ensure similar safeguards for their residents.* MA201 requires that all personal data – social security and driver's license numbers, financial account data, credit card information, for example – must be protected and encrypted "at rest and in transit." Additionally, businesses with Massachusetts employees bear the burden of attesting to such compliance.

Once again this important standard applies equally to Deltek or Intuit systems running on site in your server room, or remotely at a hosting center. With identity theft America's fastest growing crime, clear internal and audited controls to protect employee data are more important than ever.

D. "High-Impact Data" Controls. Increasingly, the federal government is promulgating standards for the access and control of data it considers to be "high-impact." Among the alphabet soup of relevant regulations are CMS (Centers for Medicare and Medicaid Services), of concern to businesses with HHS contracts, DISA (Defense Information Systems Agency), for organizations that access and maintain Defense Department or Veterans data, and FISMA (the Federal Information Management Security Act), which applies to data generated by federal entities and maintained by third parties.

The Department of Commerce among others has outlined 17 security-related measures that are required to protect "the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems." If your organization handles any such government data in its Deltek or QuickBooks system, high-impact data requirements most likely apply. At TBS, high-impact data compliance for CMS and DISA are baked into our hosting platform, and included in the scope of our annual audit.

E. Finally, it's critical to understand that the old SAS 70 Type II regime that potentially covered many of these rules and controls was discontinued by the American Institute of Certified Public Accountants in 2010, because the AICPA found its application to be ambiguous and often misrepresented.

Under the SAS 70 system, cloud services and hosting providers were free to define the scope of their own audit (or lack thereof) to meet various regulatory controls. This year, the new SSAE16-SOC2 system, which has replaced SAS 70, requires cloud providers to follow industry-standard guidelines for each regulatory regime as defined by the AICPA. If you're considering a hosting provider that boasts about its SAS 70, you might want to think twice. And, the new SSAE16-**SOC1** standard does NOT apply to Cloud Hosting providers, as SOC1 does NOT include security controls. As you survey the hosting marketplace, you'll find some providers trumpet their SOC1. SOC1 is the wrong assurance standard, but some providers cling to it because SOC2 is likely too hard for them to attain.

At TBS our hosting platform is built so that ALL customers receive the benefit of our robust SSAE16-SOC2 environment (our annual audit review and attestation period begins in July and ends in December). This means that all organizations that host their Deltek or QuickBooks data and applications with TBS meet the numerous financial IT control mandates required by GSA or DCAA audits, and MA201, ITAR, and other high-impact data regulations, even Sarbanes-Oxley.

The bottom line? When it comes to Deltek Cloud Hosting, not all compliance environments are the same, and a "SAS 70 Type II facility" or an "SOC1 environment" are simply not good enough. Safeguarding and securing your most important and sensitive financial data requires much, much more than that. So, ask your hosting provider for a copy of their annual audit report, and review their compliance scope "Control Objectives." And take note of whether that report is from their facility or the business itself.

Cloud compliance requires more than hot air. It demands cold, hard facts.