



Abt Associates' Analytic Computing Environment (ACE)

Secure, Full-Featured Analytic Computing in the Cloud

Abt Associates built its Analytic Computing Environment (ACE) to meet all of its clients' data science and analytics challenges. ACE rests on the twin foundations of **full-featured analytic capacity** and **data security and compliance**.

Full-featured Analytic Capacity

At Abt Associates, all analytic activity occurs in our ACE environment. Data are centralized, so our project analysts can access them with any tool within this secure environment. ACE is equipped with a full complement of state-of-the-art quantitative, qualitative, geospatial, visualization, and survey/data collection tools, to meet diverse project analytic needs. Using shared project folders, our project analysts can collaborate, review one another's work, and always use the best tools for any job. The efficiency of our approach makes it unnecessary to move data around or to add or upgrade software on users' desktop computers, preventing delays.

Our ACE platform covers the full data lifecycle, from collecting/acquiring survey and administrative data, through data cleaning, analytic programming and analysis, data visualization and dissemination, and long-term data retention or data destruction

To apply efficient, high-quality solutions to our data analytics, Abt Associates maintains a repository of tested, re-usable code. Our analytic code for each project is stored in a code repository, which provides strict version control. We also use the most advanced versions of our core analytic tools and deploy them on high-performance, redundant servers in the cloud.

ACE is built on Amazon Web Services (AWS), the leading cloud service provider. AWS guarantees to be available more than 99.99% of the time, and Abt project analysts can access the system from any location. Using AWS, we can easily increase the capacity of our servers to process larger or concurrent jobs more quickly. Abt is an AWS

Advanced Partner; this status testifies to our expertise in maintaining this platform and gives us direct access to AWS staff and expertise.

Data Security and Compliance

Supporting all project activities in a single environment minimizes risks inherent in moving data and storing them in multiple locations. ACE complies with HIPAA, FERPA, and FISMA Moderate standards. AWS addresses the FedRAMP security control requirements that are aligned to the NIST 800-53, Rev. 4 Security control baseline for Moderate impact levels. ACE uses only AWS components that are fully FedRAMP authorized, and we strictly adhere to FISMA Moderate compliance controls for all applications.

End users are the most vulnerable point in any secure system. We restrict access to project data; only authorized users working on a particular project have access to the data for that project. To further minimize this risk, authorized users access ACE through two-factor authentication, including complex passwords they must change every 60 days. After users log in, the system presents them with a virtual desktop, allowing them to do all of their work in the secure environment. And we ensure personally identifying information (PII) or other sensitive data don't escape. Before users can copy data out of the secure environment, the data are first scanned by the Symantec Data Loss Prevention tool, which uses advanced algorithms to detect such information. If users need to transfer sensitive data to or from a client or third party, they must use the FedRAMP-compliant data-sharing tool Huddle, or an alternative mechanism that the client has specifically approved.

CORE ANALYTIC TOOLS AVAILABLE ON ACE

Quantitative

- SAS
- Stata
- R Studio
- Python/Anaconda
- SPSS
- MatLab

Qualitative

- NVivo

GeoSpatial

- ArcGIS Pro
- ArcGIS Server
- ArcGIS Image Server

Visualization

- Tableau
- QlikSense

Survey/ Data Collection

- Confirmit
- Sytel

Databases

- SQL Server
- PostgreSQL



Abt Associates' Analytic Computing Environment (ACE)

Secure, Full-Featured Analytic Computing in the Cloud

Additional technical security features include encrypted storage, intrusion detection systems, advanced anti-virus protection, and audit log aggregation systems. A Network Operating Center (NOC) monitors ACE seven days a week, 24 hours a day, and expert security staff continuously review audit logs, conduct regular scans, and apply patches. A formal configuration control board reviews all changes to the ACE environment before they are implemented.

We back up project data on ACE in two ways: We use AWS Snapshots to back up complete pictures of a disk; and we maintain encrypted, file-based backups stored both on AWS and at a remote data center outside of AWS. This allows us to restore single files quickly and ensures data durability in the highly unlikely event of a long-term disruption to the AWS infrastructure.

Federal clients with data on ACE include the U.S. Agency for International Development (USAID), Centers for Medicare and Medicaid Services, Centers for Disease Control and Prevention, Social Security Administration, Environmental Protection Agency, and the U.S. Departments of Justice, Housing and Urban Development, Labor, and Education. ACE also holds data for foreign governments, state and local agencies, foundations, universities, corporations, and non-profits. These include the United Kingdom's Department for International Development; the Massachusetts Department of Early Education, Illinois Department of Natural Resources, and New York City Department of Health and Mental Hygiene; the Bill and Melinda Gates Foundation and the Conrad Hilton Foundation; John Hopkins University; General Dynamics; and Compass Working Capital and Citizen Schools.

