Cloud Computing Primer

This document provides basic information for clients considering deploying ProjStream's BOEMax, EVMax, or MaxTeam software tools in the cloud.

What is Cloud Computing?

A common definition is on-demand computing services that are delivered over the internet where you pay a cloud service provider (CSP) a subscription fee or when you use resources.[1] The CSP maintains a virtualized pool of resources from raw compute power and database storage to applications and developer tools. The advantage is scalability and agility. The CSP uses automated provisioning to tap those resources in real time to support changing workload demands.

What Are the Benefits of Cloud Computing?

What benefits are important to you depends on what you want to achieve. It also depends on what types of services or products your company provides. For some, moving to a cloud environment frees information technology (IT) personnel to focus on internal business needs instead of maintaining a data center. For others, it is a way to reduce the time to market for a new product or software application. They can take advantage of new advanced cloud services as well as the latest trends in software development such as devops to meet business demands for speed, agility, and responsiveness.

Often cited benefits of cloud computing include:

- *The ability to scale up or down dynamically*. This is sometimes referred to as "elasticity." This could be raw computing power or storage to handle a surge in data volume. It could also be a fluctuating number of users accessing an application.
- *You pay for what you use*. Because cloud services can scale dynamically, it can be cheaper to rent your IT infrastructure instead of building and maintaining your own. The cloud services are an operational expense instead of a large capital expenditure for a physical IT infrastructure that must be maintained and quickly becomes obsolete.
- *Security*. Qualified CSPs are certified they meet US government security requirements defined in the Federal Risk and Authorization Management Program (FedRAMP). CSPs have personnel dedicated to mitigating the broad spectrum of evolving cyber threats and use methods to secure the data such as encryption. In comparison, physical IT infrastructures maintained in-house that fail to keep pace with hardware and software vulnerabilities create significant security risks for a company. The ability to proactively combat all types of cyber threats and vulnerabilities is an absolute business necessity.

- *Resiliency*. Because cloud services are distributed, scalable, and redundant in nature, CSPs can quickly overcome infrastructure degradation, operational outages, or significant cyber events to ensure business continuity. This failover feature means the CSP automatically switches to a secondary system should the primary system fail minimizing any impact to system users.

Is Cloud Computing Secure?

Even though security is often listed as a benefit to cloud computing, many companies remain concerned about security risks. A recent IDG cloud computing survey[2] found that 34% of companies have security concerns. Qualified CSPs have proven themselves much less susceptible to attack than the average enterprise data center because they must proactively maintain their FedRAMP certifications and demonstrate they provide a secure managed solution.

Security is a shared responsibility between you and the CSP. The greater security risk may be your existing systems, how data are stored, and user authentication. Internal security policies and identity management often need to be enhanced and proactively managed to properly secure the data and services. Security practices need to evolve to integrate effectively with the range of cloud infrastructure or applications your company plans to deploy over time.

Cybersecurity processes and practices must be in place to adequately protect your company's proprietary information, intellectual property, technical information, and information systems from unauthorized disclosure or malicious attackers whether your systems are internal or in the cloud. This has become a matter of economic and national security for the US industrial base.

Moving to the Cloud as a Business Strategy

Survey results indicate cloud adoption and spending is increasing. According to the same IDG survey, nine out of ten companies have already moved at least some of their applications to the cloud or plan to do so in the next 12 months. The average investment in the cloud rose in 2018 to nearly 36% from two years ago.

Your company may have already started moving infrastructure or applications to the cloud, often as part of overall business initiatives to achieve process agility – the ability to quickly respond to internal and customer demands.

The US federal government, and in particular, the DoD is no different. They know they need to embrace the cloud to ensure mission success and mitigate cyber security risks. The DoD recently published a Cloud Strategy[3] document emphasizing their commitment to the cloud and their need to view initiatives from an enterprise perspective. The DoD intends to implement a Joint Enterprise Defense Infrastructure (JEDI), for the majority of systems and applications. This will help them to take advantage of economies of scale, provide a core of common services, proactively address cyber challenges, and leverage data analytics so personnel can make time-critical decisions.

What Are the Requirements for US Federal Government Contractors?

For contractors with federal government contracts that want to take advantage of could computing, there are a number of compliance and security control standards that apply. Cyber security must be a top priority for all companies.

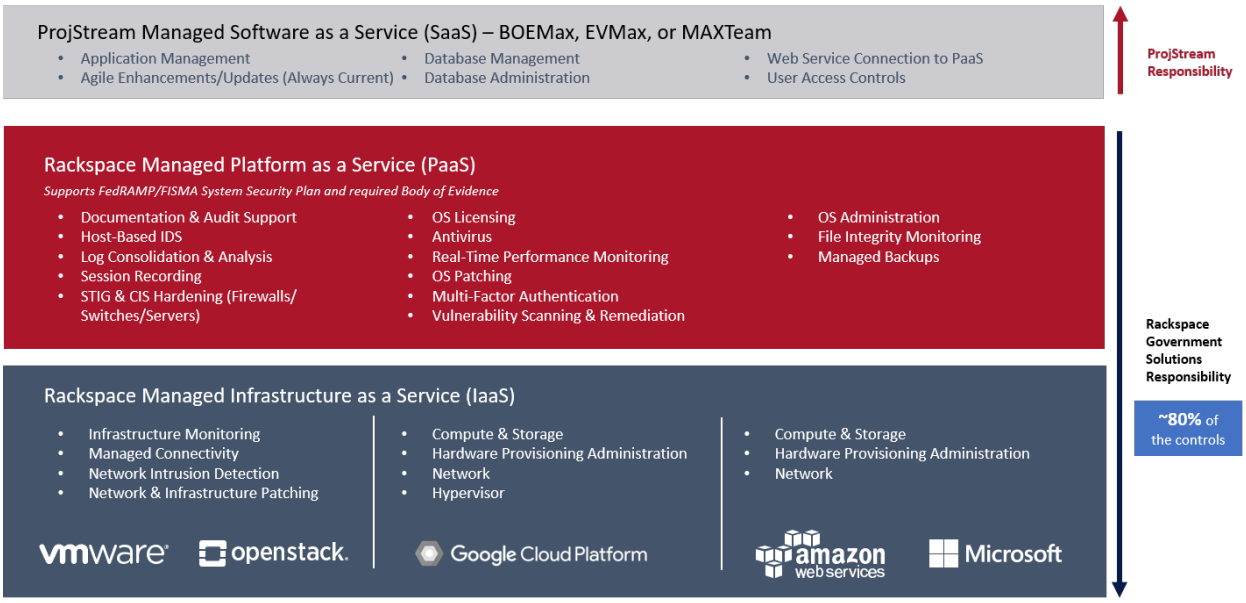
A few of the primary standards and regulations to be aware of include the:

- *Cybersecurity Maturity Model Certification (CMMC)*.[4] The Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)), established this framework as a means to verify and certify a contractor has implemented the necessary processes and practices to achieve a defined level of cybersecurity capability. CMMC merges a number of cybersecurity control standards into a single, more comprehensive standard. This includes NIST SP 800-171, and the DFARS Clause 252.204-7012. CMMC requires the defense industrial base to become certified once the CMMC is fully integrated into the DoD acquisition process. By 2026, all new contracts will specify the level of CMMC certification that applies. Compliance will be enforced and mandatory for all contract awards.
- *Federal Risk and Authorization Management Program (FedRAMP)*. FedRAMP was created to support the government cloud computing plan to facilitate the adoption of cloud services among federal agencies with a single, standard security requirements accreditation for a CSP. All federal government cloud systems must comply with the Office of Management and Budget (OMB) mandate to convert to FedRAMP standards. FedRAMP is one standard that encompasses many such as FISMA, HIPAA, NIST 800-53, and NIST SP 800-171. The FedRAMP certification process is intensive with rigorous compliance requirements a CSP must proactively maintain. The benefit for a CSP is they are able to work with all government agencies and non-government customers may be more confident in a certified CSP's approach to security.
- *Federal Information Security Management Act (FISMA)*. This legislation was signed into law as part of the Electronic Government Act of 2002. It requires government agencies to ensure the security of data in the federal government and to minimize risks with proactive security programs.
- *International Traffic in Arms Regulations (ITAR)*. The intent of this regulation is to control the export and import of defense-related articles and services on the United States Munitions List (USML). The goal is to prevent the disclosure or transfer of sensitive information to a foreign national. All manufacturers, exporters, and brokers of defense articles, defense services, or related technical data must be ITAR compliant. The responsibility lies with the manufacturer or exporter to take the necessary precautions and steps to certify that they are meeting ITAR compliance requirements. For a company that must be ITAR compliant, internal controls must be in place to ensure data in the cloud is managed by US persons in US locations.

What Are the Different Types of Cloud Delivery Models?

There a variety of cloud computing services in the marketplace. The most common types include *software as a service (SaaS)*, *platform as a service (PaaS)*, and *infrastructure as a service (IaaS)*. A CSP may provide a single type of service or a range of services. Each type of service has different roles organized in a stack.

The following image illustrates this stack with ProjStream managing the SaaS and Rackspace,[5] a FedRAMP certified CSP, managing the PaaS and IaaS.



- At the bottom of the stack is IaaS. This includes the basic services that can be rented such as physical or virtual servers, storage, networking, and other options depending upon the CSP. Amazon Web Services (AWS) was the first IaaS provider and remains the leader followed by Microsoft Azure, Google Cloud Platform, and IBM Cloud. The IaaS provider can help you comply with ITAR requirements to control where the data resides or who can access the data.
- The next layer up is PaaS. This layer includes shared development tools, processes, or services developers need to build applications including middleware, database management, and operating systems. As illustrated above, an important service here is maintaining FedRAMP security compliance and certification.
- At the top of the stack is SaaS. This is the delivery of business applications as a service. An example of SaaS is Microsoft's Office 365. ProjStream's tools can also be deployed as a web service. The underlying hardware and operating system are irrelevant to the end users. They access the application using a web service or through a browser. It is often purchased on a per-seat or per-user basis.

Other common types of services include:

- Private clouds. These downsize the technologies used for IaaS public clouds so they can be deployed and operated within a company's data center. The benefit is the company can take advantage of automated provisioning of virtual resources. However, only internal users experience it as a cloud computing service.
- Hybrid clouds. These integrate a private cloud with a public cloud. The types of integrations can vary depending on the business needs.

The IDG Cloud Computing Survey provides other insights into what companies are doing. For example:

- Organizations are using a mix of cloud delivery models. Currently the average environment is 53% non-cloud, 23% SaaS, 16% IaaS, and 9% PaaS. In the next 18 months, non-cloud delivery will account for less than a third (31%) of the average IT environment, SaaS 33%, IaaS 22%, and PaaS 14%. SaaS will be in use at 95% of companies, IaaS at 83%, and PaaS at 73%.
- Forty-two percent of organizations are using multiple cloud providers. The top two benefits of a multi cloud strategy are increased cloud options (59%), and easier and faster disaster recovery (40%).

Deploying Cost Estimating or Project Control Tools in the Cloud

ProjStream can support a number of different scenarios to deploy our software tools in the cloud. For example:

- If your company has established a cloud environment with one or more CSPs, ProjStream works your internal IT personnel to add the ProjStream business application to your cloud environment. You determine whether you want ProjStream to manage the tools for you (function as SaaS) or your IT personnel manage the tools.
- ProjStream managed SaaS plus a CSP managed PaaS/IaaS. We deploy our software as a service for you where we contract with a FedRAMP certified CSP such as Rackspace to handle the security and infrastructure layers.

The SaaS plus managed PaaS/IaaS model often works well to address internal IT resource limitations or to lower the cost of the ownership. Another example: a small company that has a one-off three-year project with earned value management system (EVMS) requirements and needs a tool to produce contractual performance reports for a given timeframe.

What Does it Mean to be Optimized for the Cloud?

You do have choices for proposal management, earned value management, and project cost management tools. A consideration to include in your requirements list is whether the tool is designed to support cloud environments.

ProjStream is an agile software development company that has embraced the cloud computing delivery model. We can support traditional and cloud computing environments. The software can be deployed on a local computer, on a server, or as a web service.

Applications optimized for the cloud computing delivery model or “cloud-native” applications:

- Are designed to run in cloud environments. They can scale up or down on demand because of how the application is built, delivered and operated.
- Use agile and scalable components like containers. They are modular with many functions broken down into microservices. That means it is easy to update the software. The benefit? The application is always current.
- Are not tied to the infrastructure and can work in a virtual environment. The application can run in a highly distributed manner and maintain its “state” (the application knows where it is in the process of things) independent of the elastic nature of the underlying infrastructure.

Legacy software designed for a client/server environment cannot exploit the advantages of the cloud computing delivery model. The software is monolithic in design – the exact opposite of applications designed for the cloud. Updates and enhancements are a major event – they are often released as "patches" or new versions that break the rigid connections with the underlying infrastructure. The software vendor may put a browser front-end on a desktop tool so it appears to function as web service. The down side is performance degradation and security. "Lifting and shifting" a legacy application may be a stop-gap measure. However, it limits your options in the future. At some point it will matter as more applications move to the cloud.

Terms and Definitions

CMMC	Cybersecurity Maturity Model Certification (CMMC). Similar to other maturity models, it provides a framework of processes and best practices a contractor follows to achieve a defined level of cybersecurity capability that can be independently verified by an approved CMMC third party assessment organization. Created to merge all the different cybersecurity requirements and standards into a single standard that is more comprehensive.
CSP	Cloud service provider. There are different types of cloud services. See the definitions for software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).
Devops	A combination of "development" and "operations." The objective is to align the priorities between the development and operations teams to reduce the time to market with a higher quality product focused on customer needs. Devops encompasses the organization structure, practices, and culture so teams have a single mindset of responding faster to business needs. It combines rapid agile development and innovation that is balanced with security and operational needs.
DFARS Clause 252.204-7012	Safeguarding Covered Defense and Cyber Incident Reporting. DoD contractual clause that spells out contractor requirements to protect information and information systems as well as reporting cyber incidents. Cites NIST SP 800-171.
Failover	A means for ensuring high availability of a critical resource such as a computer system, involving a parallel, backup system so that when there is a detected failure of the primary system, processing can be automatically shifted over to the backup.
FedRAMP	Federal Risk and Authorization Management Program. Created to standardize the approach for assessing and monitoring the security of cloud products and services for US federal government agencies. CSPs with a FedRAMP certification have demonstrated they have a unified risk management process in place that includes agreed upon security requirements.
FISMA	Federal Information Security Management Act. US legislations that defined a comprehensive framework to protect government information, operations, and assets against natural or human threats. It was signed into law as part of the Electronic Government Act of 2002. Agencies must ensure the security of data in the government with annual reviews of information security programs. The intent is to keep risk at or below specified levels in a cost-effective, timely, and efficient manner.
IaaS	Infrastructure as a service. The foundation layer for cloud services. Typically includes an array of servers for computing and data storage, networks, and other services.
ITAR	International Traffic in Arms Regulations. Controls exports from the US of defense related articles. Non US citizens cannot have physical or logical access to articles stored in an ITAR environment unless a special authorization or exemption is in place.

NIST 800-53	Provides a catalog of security and privacy controls for federal information systems and organizations. It is a mandatory federal standard developed by NIST in response to FISMA.
NIST SP 800-171	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. This publication provides federal agencies and other organizations with a set of recommended security requirements for protecting the confidentiality of controlled unclassified information (CUI).
PaaS	Platform as a Service. The middle layer for cloud services. Typically includes operating systems, development tools, middleware, database management, and other services. Security monitoring and controls are an important component of this layer.
SaaS	Software as a Service. The top layer for cloud services. This is the layer visible to the end users of an application.

References

1. If you want to learn more, a general search for cloud computing produces a number of sources for information. One of many information sources include articles on the InfoWorld web site with an abundance of links to related topics.
   Visit https://www.infoworld.com/article/2683784/what-is-cloud-computing.html
2. 2018 IDG Cloud Computing Study. Visit https://www.idg.com/tools-for-marketers/2018-cloud-computing-survey/
3. DoD Cloud Strategy, December 2018.
   Visit https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF to download a copy.
4. For more information about the Office of the Security of Defense CMMC initiative, visit: www.acq.osd.mil/cmmc/.
5. Rackspace is one example of a CSP. For more information, visit https://www.rackspace.com/