A Special Report

Cloud Computing

Report on Cloud Computing used in the Aerospace and Defense Industry
Important Disclaimer: The Aerospace Industries Association of America, Inc. (“AIA”) has no intellectual property or other interest in this document. By developing this document and making it freely available to anyone, AIA assumes no responsibility for this Use-case scenario’s content or use, and disclaims any potential liability associated therewith.
## Contents

1. Statement on Previous Conclusions ............................................................................................................. 4  
2. Aerospace and Defense Requirements on Cloud Computing ........................................................................ 4  
   2.1. Reliability of Service Requirements ........................................................................................................ 4  
   2.2. Requirements for Tracking Sensitive and Restricted Documentation ..................................................... 5  
   2.3. Encryption Requirements ........................................................................................................................ 5  
   2.4. Long-Term Archival and Retrieval ........................................................................................................... 5  
   2.5. Storage Requirements ............................................................................................................................ 6  
3. Architecture – References to Standards ........................................................................................................ 6  
   3.1. National Institute for Standards and Technology (NIST) Strategies ....................................................... 6  
      3.1.1. The NIST Role .................................................................................................................................. 6  
      3.1.3. The Federal Risk and Authorization Management Program (FedRAMP) ....................................... 7  
      3.1.4. Combined Conceptual Reference Diagram NIST Special Publication 500-292 .............................. 8  
4. Cloud Adoption and Use Strategies .............................................................................................................. 8  
5. Improvements in Technology ........................................................................................................................ 9  
6. Service Availability ....................................................................................................................................... 10  
   6.1. Service Level Agreements – Key Aspects and Validation ....................................................................... 10  
7. Recognition of Security Concerns .............................................................................................................. 10  
8. Cloud Migration Strategy ............................................................................................................................ 11  
   8.1. Business Objectives ............................................................................................................................... 11  
   8.2. Service Requirements .......................................................................................................................... 11  
   8.3. Operational/System Requirements ....................................................................................................... 11  
   8.4. Strategic Roadmap .................................................................................................................................. 11  
9. Mature Applications ..................................................................................................................................... 11  
   9.1. Human Resources ................................................................................................................................... 12  
      9.1.1. Benefits ........................................................................................................................................ 12  
      9.1.2. Risks ............................................................................................................................................ 12  
   9.2. Administration and Accounting ............................................................................................................. 13  
      9.2.1. Travel Booking and Expense Processing ......................................................................................... 13  
      9.2.2. Accounting .................................................................................................................................. 13  
   9.3. Customer Relationship Management .................................................................................................... 13  
10. Business and Technology Gaps .................................................................................................................. 13  
11. Barriers to Wider Exploitation .................................................................................................................... 14  
12. Risk Assessment and Mitigations .................................................................................................................. 14
13 Recommendations for AIA Action

13.1 Potential Deliverables

Endnotes
1 Statement on Previous Conclusions
In 2010, the Aerospace Industries Association (AIA) E-Business Steering Group (EBSG), and the Electronic Enterprise Integration Committee (EEIC) published an authoritative report assessing the impact of disruptive technologies such as Cloud Computing, Social Networking and Consumerization on the aerospace and defense industry.¹ This report provided a consolidated, comprehensive review of the benefits, risks and viable mitigations of these new technologies, taking into account the complex security requirements of the aerospace and defense industry.

Some of the elements reviewed include the following:

- Characteristics
- Architecture
- Benefits
- Risks – Security, service interruptions and interoperability.
- Recommendations for risks and mitigations for large and small companies.

In the report, Cloud Computing was recognized as a technology that offers flexible access to computing resources, providing clear efficiencies, but also major challenges to the aerospace and defense industry. Protection of proprietary information when using this technology is not only business critical, but can be a national security risk if exposed inappropriately.

Cloud Computing services may be implemented at several levels of openness with associated risks:

- Private – Within a company firewall.
- Community – Restricted to a defined group of organizations, with controlled membership.
- Public – Open to all.

The use of the cloud approach brings specific issues at each level related to security, availability and interoperability of the services, which can be mitigated through appropriate action. The current U.S. Government focus on cloud initiatives means that industry needs to take a position on the use of such services.

This paper explores the various applications of Cloud Computing used by industry and government. Based on the experience to date, it identifies the latest benefits, risks and business impacts of Cloud Computing, with particular reference to portability and interoperability.

2 Aerospace and Defense Requirements on Cloud Computing

It is fundamental that the industry recognizes that the use of cloud technology does not remove the responsibility for considering information, the supporting technology, and business implications. From the perspective of the aerospace and defense industry, the following requirements are fundamental to the successful application of Cloud Computing. Most of these requirements existed before Cloud Computing was a widely available technology, and should be carefully reconsidered in the context of cloud services.

2.1 Reliability of Service Requirements
Loss of service is inevitable - whether resulting from planned maintenance or unplanned interruptions. The aerospace and defense companies, along with industry, should have an
acceptable threshold level of service reliability that is expected from service providers. Enterprises, therefore, should establish a clear Service Level Agreement (SLA) and liability for loss of cloud services, whether the provider is internal or external. The SLA should include all elements of the solutions, including applications, servers, storage, access control, authentication and network topology.

2.2 Requirements for Tracking Sensitive and Restricted Documentation

All industries create, store, manage and exchange sensitive data and information. This data includes, but is not limited to, financial, customer (individual and enterprise), and intellectual property information that must be secure and shared appropriately. The aerospace and defense industry must also be good custodians of design and operational data that may be controlled by International Traffic in Arms Regulations (ITAR) and national security classification-level for sensitive information. The industry has a need for tagging electronic documents, in addition to tagging physical documents, in order to recognize classification, export, security and intellectual property restrictions and controls.

Particular care must be taken in the event of a take-over, or change in control of a cloud provider to avoid inadvertent breaches of ITAR and national security constraints. An example of this would be the transfer of data into a foreign location and/or administration by foreign personnel.

Under ITAR, aerospace and defense companies need to be able to recognize the location of an information requester, whether it is a person, an organization or a service, for any information that is subject to export control or national security constraints. In addition, there is a need to assure the physical location of all copies of any information that is subject to export control or national security constraints. Given these requirements, companies should consider what data or information they make available through, or stored within, a cloud service. As companies have many different types of data within their respective organization, thought should be given to protecting critical data like those defined as “Technical Data” under the ITAR.

2.3 Encryption Requirements

Each business entity needs to insure that their data is encrypted to a minimal acceptable standard such as FIPS 140-2, or equivalent and higher, during the data exchange process with any outside business partner(s) and while stored in an externally hosted cloud. The best practice is that the data be encrypted prior to entering the cloud and decrypted only when arriving at the final recipient’s device.

2.4 Long-Term Archival and Retrieval

In the aerospace and defense industry, the time retention requirements for maintaining technical records and information demand a period exceeding the life of the platform with suitable archiving and recovery. Transactional and financial records may have shorter retention requirements, which are typically in the range of five to 15 years. Records for this information must have the following capabilities:

- Provenance: Producer source and consumer destination identification.
- Access tracking required to monitor current or past exposures to classified, sensitive or proprietary information and to restrict access to individuals without appropriate clearance. Data quality assurance prior to being archived.
2.5 Storage Requirements

It is important to know the physical location of all elements of the cloud solution. Disaster recovery, development and test environments could also contain sensitive information. For trade compliance purposes, it is necessary to ensure that the physical location of the cloud hosting is known, and that adequate security measures are in place to prevent theft or other loss. In addition, there are risks arising from comingling or sharing space on storage devices with other organizations, where law enforcement could seize the physical assets in the event of suspected or actual wrongdoing, preventing access to company data. The risk of business failure of the cloud service provider for any reason also dictates that use of the cloud for back-up storage should provide for data escrow. Depending on the critical nature of the data, organizations may consider creating a stored backup with two legally, separate services to protect from business failure.

For internally-hosted cloud computing infrastructures, companies will have to address the need for adequate power, space and cooling for their own physical storage.

3 Architecture – References to Standards

3.1 National Institute for Standards and Technology (NIST) Strategies

The NIST Cloud Computing Program is providing thought leadership and guidance for catalyzing Cloud Computing use within the industry and government.

3.1.1 The NIST Role

The goal of the Cloud Computing Program is to accelerate the federal government’s adoption of cloud computing by:

- Building a United States Government (USG) Cloud Computing Technology Roadmap which focuses on the highest priority USG cloud computing security, interoperability and portability requirements.
- Leading efforts to develop standards and guidelines in close consultation and collaboration with standards bodies, the private sector, and other stakeholders.

3.1.2 Draft U.S. Government Cloud Computing Technology Roadmap 03-2012

In March of 2012, NIST reported to AIA that the U.S. government’s goal is to establish a technology roadmap mechanism that utilizes Priority Action Plans (PAPs) recommended for self-tasking by the Cloud Computing Stakeholder Community.

This roadmap is explained in three, NIST publication volumes covering high-priority requirements to further USG agency Cloud Computing adoption, useful information for cloud adopters, and technical considerations for USG cloud computer deployment decisions.

3.1.2.1 NIST Priorities

The NIST has identified 10 high priority USG requirements needed to accelerate secure and effective cloud adoption. There are practical reasons why these requirements are needed for USG agencies to deploy the Cloud Computing model, which are also needed by the broad Cloud Computing Stakeholder Community. These USG Cloud Computing Technology Roadmap requirements are:
1. International, voluntary consensus-based interoperability, portability and security standards.
2. Solutions for high priority security requirements.
3. Technical specifications to enable development of consistent, high quality Service Level Agreements.
4. Clearly and consistently categorized cloud services.
5. Frameworks to support seamless implementation of federated community cloud environments.
6. Technical security solutions which are de-coupled from organizational policy decisions.
7. Defined unique government regulatory requirements, technology gaps, and solutions.
8. Collaborative parallel strategic “future cloud” development initiatives.
9. Defined and implemented reliability design goals.
10. Defined and implemented cloud service metrics.

3.1.2.2 Priority Action Plans (PAPs) Recommended for Self-Tasking by the Cloud Stakeholder Community

Such plans leverage the work completed in NIST and Complementary Cloud Community Work which:

1. Define Target USG Cloud Computing business use cases;
2. Refine and apply neutral Cloud Computing reference architecture and taxonomy; and

3.1.3 The Federal Risk and Authorization Management Program (FedRAMP)

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach utilizes a “do once, use many times” framework that will save cost, time and staff required to conduct redundant, agency security assessments.

The purpose of FedRAMP is to:

- Ensure that cloud-based services used government-wide have adequate information security;
- Eliminate duplication of effort and reduce risk management costs; and
- Enable rapid and cost-effective procurement of information systems/services for Federal agencies.
3.1.4 Combined Conceptual Reference Diagram
NIST Special Publication 500-292

Combined Conceptual Reference Diagram
NIST Special Publication 500-292

4 Cloud Adoption and Use Strategies
During the past two years, the general understanding and use of cloud services has increased. The first generation of cloud adoption is represented by consumers of cloud services applying common applications and/or systems to interface with, or to be hosted by, cloud infrastructure services. This has been realized by the success of Infrastructure as a Service (IaaS) companies. This strategy provides immediate restructuring of the computing cost and a reduction in the resources required to manage the infrastructure. However, the functionality of the systems has largely remained the same.

The second generation of cloud adoption and utilization is marked by the re-architecting and development of cloud services. Cloud platform services are engaged as a means to define and construct cloud software services. An inherent challenge to this is that the development methodologies employed to construct web applications may require rethinking to accommodate the speed and quality of cloud services being produced using cloud platforms. The software development methodology used for constructing web/Internet applications is based largely on theory established during the client/server paradigm. The agile development approach has substantially improved the cycle time of core software development. These changes enable the development/concept/validation of a solution to be performed by the business analyst. A restructuring of the software development lifecycle will be needed to accommodate the empowered business analysts. The development of second generation cloud services is shifting toward a consolidation of development platforms that new services are being designed to work with. As companies reduce the size of their information technology and software development
organizations, a greater dependency will emerge to use these platforms. This effect will be similar to the consolidation that occurred with operating systems and web browsers.

One question that needs to be considered is whether or not there will be industry-specific cloud platforms, which will provide specialized services specific to the aerospace and defense industry. There are existing proposals from the Network Centric Operations Industry Consortium - NCOIC® (https://www.ncoic.org/home/) and other industry bodies that there will be a need for a service or grouping of services for current and emerging cloud platform capabilities, and that these services will challenge the current methods and capabilities to design, develop and deploy solutions in the cloud.

5 Improvements in Technology

In most use cases, a form of cloud implementation may reduce related Information Technology costs while decreasing time to service. Cloud Computing is one of the few technologies that is improving the time to value realization, resulting in total cost reductions. Time to service is what the industry calls agility. A business service, such as “Order to Build,” can be executed twice as fast with less development time, enhancing agility and time to service. It is not evident that all organizations understand Cloud Computing Service-Oriented Architecture (SOA) models, nor are they adopting them.

Cloud Computing can be defined as both a policy-based operations service with a provision portal which connects to libraries or service catalogs, or as an automated provision engine accessible from either the policy-based service engine or from the portal. Based on this definition, the emerging technologies that will have the biggest impacts are the following:

1. Virtual Desktop Infrastructure (VDI) technologies that allow the service engine to run better.
2. Policy engines that look at actual workload to create policy.
3. Correlation engines that are content-aware versus those that use Boolean logic.
4. Security at the Advanced Persistent Threat (APT) level and at the authentication level. Security Event and Intrusion frameworks are an emerging technology area with significant advances, especially in the pretesting area. One of the actual top uses for the cloud is Testing as a Service (TaaS), in use case scenarios.
5. Advance service engines and automation engines, which are the heart of cloud offerings.
6. Emerging, unified data models and tool compatibility for operations.
7. Emerging technologies for transaction and invoicing engines based on usage.
8. Open source service operation engines and resources management systems.
9. Re-purposed technologies on portal and customer presentation technologies.
10. Advances in the High Performance Computing Technology. These technologies are advancing exponentially (Moore’s Law), so that the price per unit of performance is very attractive. There are implications on release management and data management. The dollar cost advantages as applied to specific cloud work load are significant.
11. Authentication as a Service (AaaS) is seeing emerging technologies.
12. On the network side, 4G technologies utilizing Long Term Evolution (LTE) technology are having larger impacts than expected. These low-cost, anywhere, high bandwidth network services, enable business service to edge devices, and expand their presence
dramatically. Coupling these network platforms with new technologies in WAN Acceleration and Secure Content Cache offer potential answers to difficult use cases.

13. Facilitating enterprise data mining.

6 Service Availability

It is important that the user and service provider define acceptable levels of service availability and capability in contractual agreements.

The Cloud Standard Customer Council (CSCC), an end user advocacy group, has offered guidance that users and providers can reference to assist them in developing their agreements. This guidance provides necessary elements of a SLA for Cloud Computing, and offers interested parties insight on what to be aware of when entering into an SLA with a provider. The guide suggests elements and requirements that can be satisfied through open standards, including availability of service, response times and security.

6.1 Service Level Agreements – Key Aspects and Validation

Risk mitigation strategies depend on agreements between the company and the cloud provider. Violations of the agreements must have appropriate consequences in order to ensure that there is the motivation and/or just compensation needed to truly mitigate the risks of unintended disruptions of service. These disruptions could prevent the client from accessing their data and block them from transacting business. Risk of the potential disruptions should be mitigated through the use of alternate storage.

7 Recognition of security concerns

Security issues in the cloud include, but are not restricted to:

- Unauthorized release of data;
- Data spills/leakage/exfiltration;
- Unauthorized data mining;
- Loss of data due to seizure of hardware;
- Unauthorized access;
- Hacking; and
- Movement of data outside of the country.

Information assurance standards contained in NIST Special Publication 800-53 are the standard for information security controls, while ISO 27000 should be reviewed and assessed on how they apply to cloud applications. SLAs need to include agreed upon levels of security, response to data spills and accessibility for post event interrogations.

There is a new CloudAuthZ Technical Committee within the Organization for the Advancement of Structured Information Standards (OASIS) that is focused on the development of security standards and practices for authorization within the cloud.
8 Cloud Migration Strategy
There are three phases to defining a cloud migration strategy. This approach is similar to the concepts applied with any information technology change: (1) Define Business Objective; (2) Define Service Requirements; (3) Define Operational/System Requirements. The significant difference with the cloud computing is incorporating the concept of services. To derive the full value of cloud computing requires the adoption and use of a service-orientated approach. The types of cloud computing services utilized are a function of the business objective.

8.1 Business Objectives
If, for example, a business objective is to reduce capital expenses, then use of IaaS computing services as a way of hosting applications would be an appropriate strategy. This approach may limit a business from leveraging other platform and software cloud computing services, which is an important concept to consider in developing an overall cloud services utilization plan. An enterprise architect, working closely with the business, will be able to anticipate and provide strategic guidance.

These business objectives should be expressed in business terms. For example, reducing fixed computing or software licensing costs by making use of available software services or to support seasonal demand for computing resources by utilizing cloud infrastructure services, and terms of capabilities that are utilized by the business to accomplish specific tasks.

8.2 Service Requirements
Services requirements are defined as a decomposition of the organizational activities related to the business objectives. Generally, a functional approach is taken to identify common processes that are utilized within the organization. Common functions that are supported by cloud services include financial and human resources activities. There are some functions that are unique to the aerospace and defense industry, and not as commonly available as cloud services, although a few companies are transitioning existing industry-specific applications to cloud services, thereby allowing for dynamic utilization of the required functionality.

8.3 Operational/System Requirements
The operational and system requirements are a rational decomposition of the service requirements. These formulate the system requirements that the cloud Platform as a Service (PaaS) and IaaS will be required to provide.

8.4 Strategic Roadmap
The convergence of business need and availability of the service allow for the construction of a strategic roadmap that is used to coordinate the implementation and utilization of cloud services. This roadmap becomes the baseline for the planning of resources and communication to sponsors and executives.

9 Mature Applications
There are many examples of mature business activities that have been reinvented using cloud computing, including functions such as Human Resources, Accounting, and Customer Relationship Management (CRM). Other applications could also benefit using cloud computing.
9.1 Human Resources

Human Resources and enterprise administration have been using cloud and cloud-like services for several years. These services, formerly administered through paper forms and information booklets, can now be done through online services and administered by the employee. Examples of services that can be administered by human resource professionals or self-administered and managed by the employee are:

- Retirement plans
- Benefits administration
- Insurance
- Health care providers, such as Health Management Organizations
- Commuting benefit providers

Employers are empowering their employees to access their individual information with service providers rather than have the employee either work through the HR administrator or with customer service at the benefit service provider.

9.1.1 Benefits

The employer benefits from fewer HR resources being required to administered for individual employee needs. The advantage for the employee is that they have direct access to information such as:

- Current and past payroll statements
- Retirement statements
- Flex care administration
- Leave tracking
- Employee Benefits

9.1.2 Risks

The employee’s personal and private information is stored with a third party service provider which, if not controlled, could pose a security risk. The location where this information is stored and who will have access to it is unknown to the employee and access credentials could be compromised. Employees are also responsible for maintaining additional credentials. These personal types of information include, but not limited, to:

- Individual or family’s medical history and condition.
- Individual’s compensation, accrued vacation and sick leave, as well as patterns in employee’s usage of leave.
- Personal identity information: financial information, national identification numbers, and employee’s family information.
- Health Insurance Portability and Accountability Act (HIPAA)
- Safe Harbor and other privacy regulations
- Management of employee’s retirement accounts. Nefarious activity could compromise the employee’s account and even the service provider’s liquidity.
9.2 Administration and Accounting

9.2.1 Travel Booking and Expense Processing
Travel bookings can be made through cloud based services, which combine multiple service components to cover all aspects of the reservation services, including trade-offs for best overall value. The subsequent travel expense process can be more efficient than traditional practices for this activity since they can be processed in real-time from anywhere, versus the employee submitting hard copy expense reports sometime after the expenses have been incurred. Other advantages are that cost accounting can be done automatically, in lieu of manual sorting by an administrator. Further advantages can be realized thought better fidelity in auditability of expense reports.

One disadvantage is that company policies will most likely require accommodating the infrastructure as a service approach to this activity. Any hardcopy of receipts would have to be submitted separately, scanned and captured locally. Security concerns would arise from service providers being able to track individuals from the company.

9.2.2 Accounting
Accounts Payable/Receivable are centralized services for managing transaction involving the payment of invoices, as well as collecting funds for goods supplied or services rendered. Accounts payable and receivable software can be accessed for managing cash transaction flow into and out of the enterprise. Transactions can be managed independent of the location and the work may be outsourced to other providers. Cloud-based applications may be utilized for this function.

The aerospace and defense companies supporting the Department of Defense use a web-based system called Wide Area Work Flow (WAWF) to manage invoices, document processing and accounting functions. For commercial aerospace, these business practices can be managed through the ATA Spec 200.

9.3 Customer Relationship Management (CRM)
CRM is a widely implemented model for managing a company’s interactions with customers and prospects. Tools like SalesForce.com have been available for some time, and are an example of an application that has competitive information which manages a company’s customer base and sales-lead pool.

10 Business and Technology Gaps
Some of the major concerns related to the use of cloud technology are:

- Security related to sharing computing power with other organizations.
- Capacity of delivering service is greater now.
- Risk of being unaware of where your data is located.
- Contractual relationship is managed by the employee.
- Casual individual or group decision making.
- Becoming a target for cyber attacks.
11 Barriers to Wider Adoption

Many enterprises are still not using Cloud Computing architecture for the management of services that involve their intellectual property or their core business, nor are they embracing cloud services for handling sensitive program information. Cloud services are currently inappropriate for classified information.

Companies are using the cloud primarily for unclassified and non-sensitive company information. Apprehension exists where risks and uncertainties remain on what will happen with their data, where the data will be stored, and whether there could be comingling of their critical data on servers that store data belonging to other enterprises.

12 Risk Assessment and Mitigations

In the 2010 report, the following risks and appropriate mitigations were covered for the aerospace and defense industry:

- Success factors
- Cost reduction
- Non-core business processes
- Commodity application
- No IPR risk
- Varying resource requirements
- Cloud sourcing
- System upgrades
- Security capability
- Non-security capabilities
- Auditability.

13 Recommendations for AIA Action

It is recommended that the AIA Electronic Enterprise Integration Committee take action to track and contribute to the development of Cloud Computing standards where necessary, and to influence their content and direction to the benefit of the aerospace and defense industry. This will ensure that these standards could be used to support the aerospace and defense industry requirements. This action should address issues of security, availability and interoperability within and between cloud service providers.

In particular, security protocols for information such as tagging requirements should be designed to be compatible with the work of the Transglobal Secure Collaboration Program. As standards and protocols related to Cloud Computing Technologies are developed, AIA needs to monitor and adopt them as appropriate.

It is recommended that the AIA advocate consistent, cost effective standards that are applied across different governmental departments and agencies to facilitate the necessary connectivity to cloud services. AIA should also promote consistent international standards for the aerospace and defense industry.
It is recommended that AIA consider the business case for establishing an aerospace and defense community environment using an external cloud service provider, as referenced in the 2010 report.

It is recommended that AIA define and publish performance standards covering specific requirements for the aerospace and defense industry. This standard practice could include minimum service levels that include conditions for addressing ITAR, and controlled unclassified information.

13.1 Potential Deliverables
Based on cloud technologies that support the requirements of the industry, it will be possible to develop recommendations on services that a vendor could use to support the aerospace industry with corresponding recommendations on service level agreements. Applications that the aerospace industry could benefit from are:

- Industry secure e-mail applications.
- Data exchange services.
- Secure e-mail exchange standard capabilities and liabilities.
- Substantive use case for utilizing a secure cloud throughout the aerospace and defense industry.

The initial deliverable for AIA’s Electronic Enterprise integration Committee would be to develop a business scenario for cloud computing based on an aerospace secure e-mail service, and identify the process flows and benefits to the stakeholders. A white paper should be published that defines the opportunity and feasibility for providing a cloud-based secure e-mail service supported by the secure e-mail standard, TransGlobal Secure Collaboration Program (TSCP) SEv1. This deliverable leverages the AIA EEIC recommendation for the adoption of this specification into a useful product for industry.

The assumption is that this application would be developed as a hosted service, with cloud-based storage and not a client-based infrastructure.
Endnotes


