

The background of the slide is a photograph of a landfill filled with numerous blue plastic bags. The image is overlaid with a semi-transparent blue filter. In the lower right portion of the blue overlay, several CD-ROMs are visible, arranged in a circular pattern, symbolizing digital data or software.

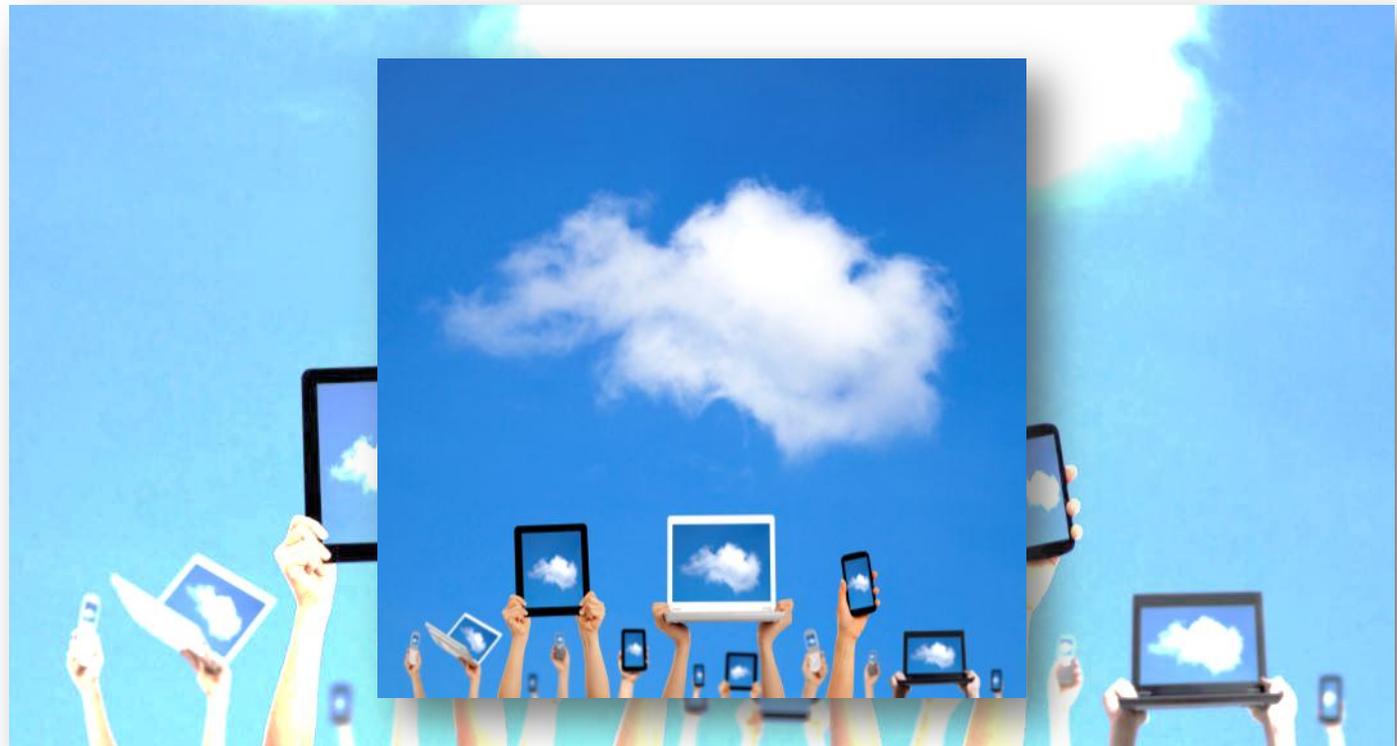
The Virtual Landfill: Disposing of Software in DoD

CM Trends 2013
August 9, 2013

Professor John Rice
Professor Tom McMannes

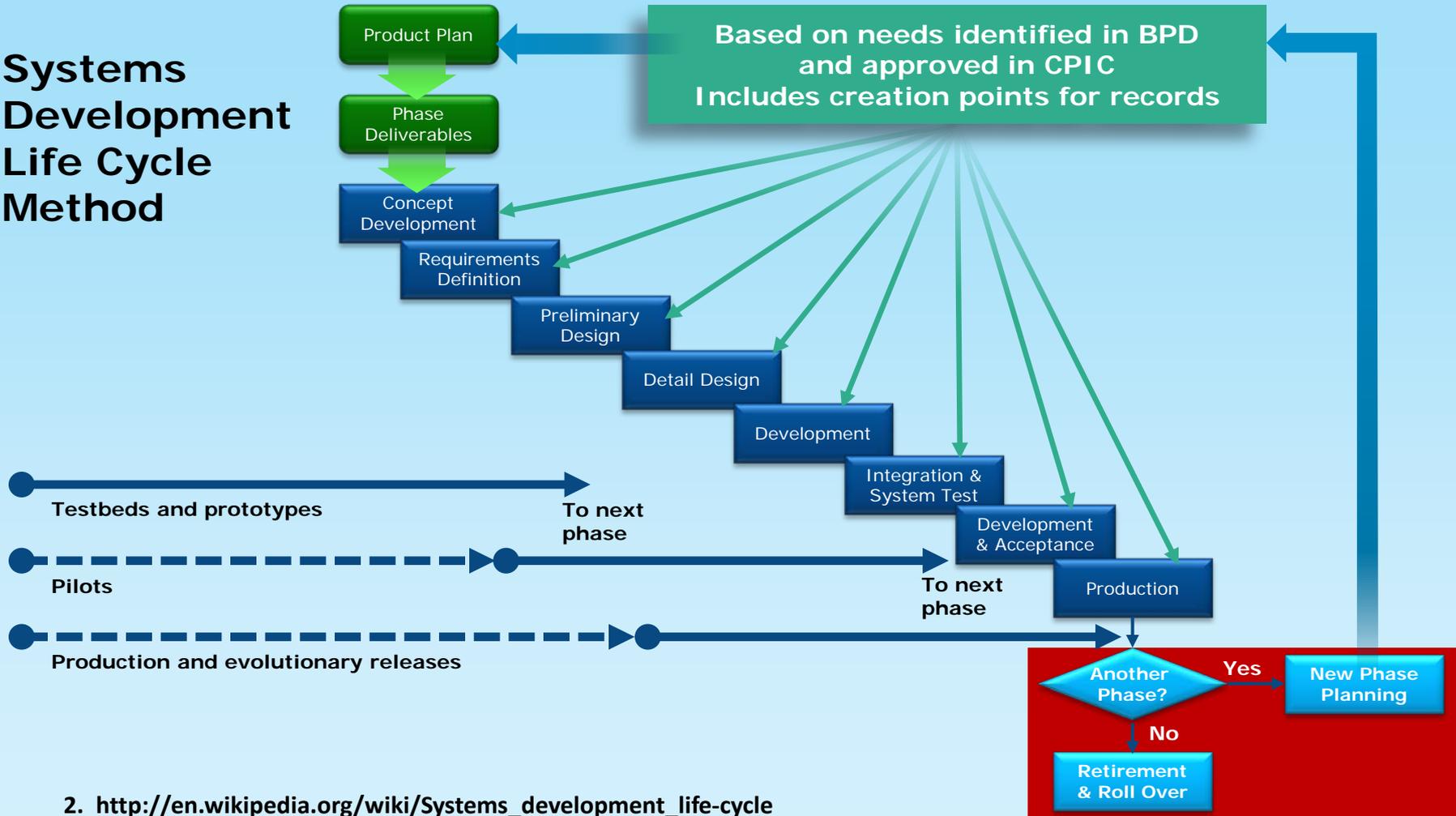
A Storm is Brewing

“Some people envision a future in which the Web becomes a massive storage cloud. A concept of data ownership will lose it’s meaning. Secrecy will cease to exist.” ¹



1. <http://computer.howstuffworks.com/cloud-computing/cloud-storage2.htm>

Systems Development Life Cycle Method



2. http://en.wikipedia.org/wiki/Systems_development_life-cycle

Definition of Software

“Computer program, procedures, and possibly associated documentation and data, pertaining to the operation of a computer system.” ³



3. DoD Open Systems Architecture, Contract Guidebook for Program Managers v1.1, June 2013

Definition of Disposal 4



- To end the existence of a system's software entity.
- Ends active support by the operation and maintenance organization, or deactivates, disassembles and removes the affected software products, consigning them to a final condition and leaving the environment in an acceptable condition.
- Destroys or stores system software elements/ products in accordance with legislation agreements, organizational constraints, and stakeholder requirements.

When Should a System be “Trashed”?



- When there is no further user requirement
- When the owner of the system is no longer willing to sponsor the system
- When an enterprise common system is mandated
- Not cost-effective to comply with new guidance

Impacts on:

- **Classification level including secret and aggregated secret**
- **Distribution of proprietary or licensed products**
- **Contractual breaches from infringement of non-disclosure agreements**



TOP SECRET

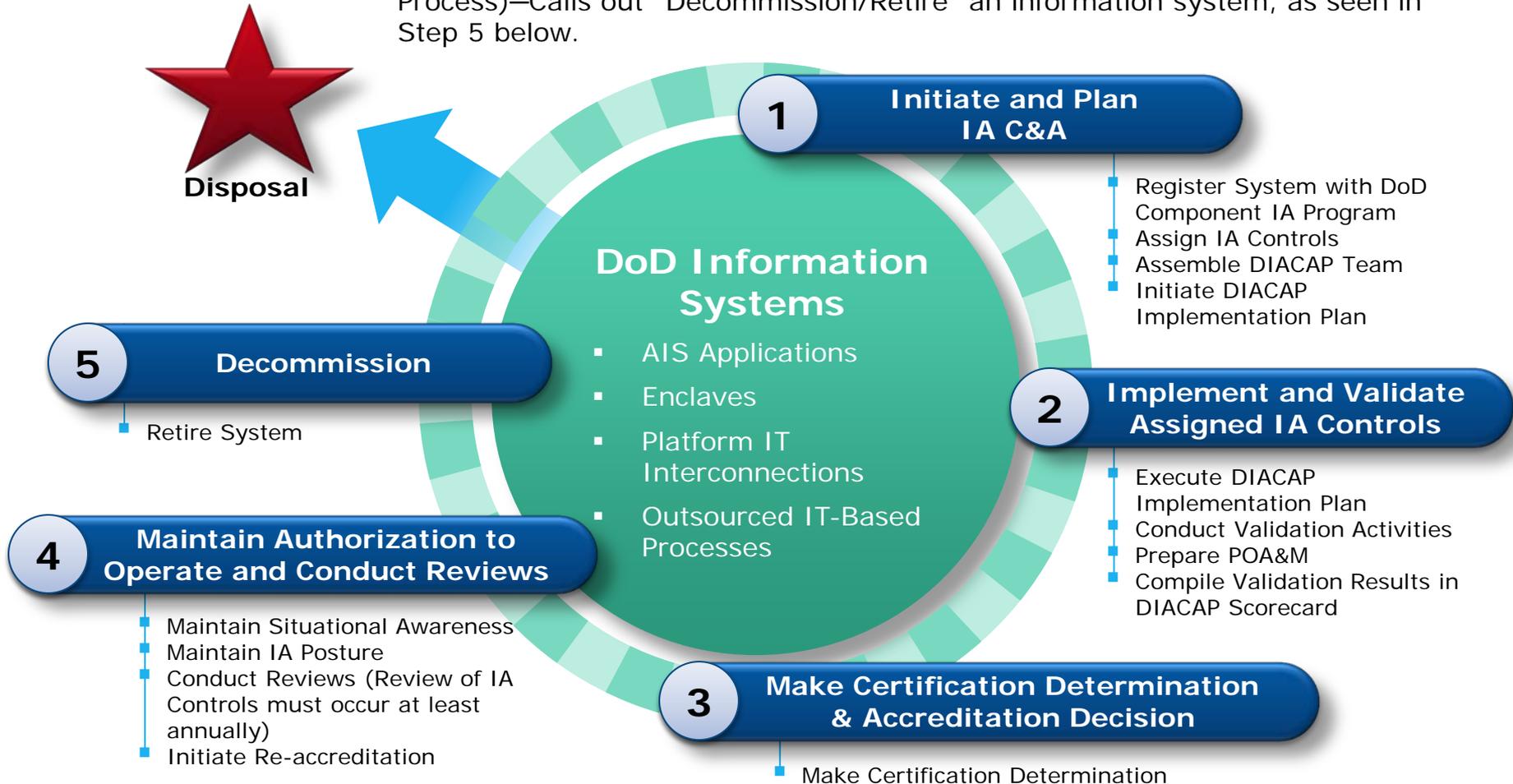


"... significant risks are also presented in the **disposal processes**. For example, an attacker could insert malicious code into a program or a microelectronics chip could be tainted and not perform as expected, or an adversary could extract valuable data from **improperly destroyed media**."

"An insurance industry stakeholder submitted that the risk of a commercial entity being sued because of **improper data disposal** is three times greater than the risk of legal action stemming from a data breach caused by loss or theft, and six times greater than from data breaches involving the loss of financial information. " 5

5. Final Report of the Department of Defense and General Services Administration: Improving Cybersecurity and Resilience through Acquisition, June 2013

DIACAP Process (DoD Information Assurance Certification and Accreditation Process)—Calls out “Decommission/Retire” an information system, as seen in Step 5 below.



Disposal of Records Per National Archives & Records Administration (NARA) Statute

Disposal of Records (44 U.S.C. Chapter 33) ⁷

§ 3302. Regulations covering lists of records for disposal, procedure for disposal, and standards for reproduction

- **§ 3303. Lists and schedules of records to be submitted to Archivist by head of each Government agency**
- **§ 3310. Disposal of records constituting menace to health, life, or property**
- **§ 3311. Destruction of records outside continental United States in time of war or when hostile action seems imminent; written report to Archivist**

7. <http://www.archives.gov/about/laws/disposal-of-records.html>

Disposal Considerations ⁸

- 
1. Obtain system owner signoff of decommission, or obtain the written decommission guidance/mandate.
 2. Update DoD system registration – DIACAP's SIP (System ID Profile) form.
 3. Notify all users/stakeholders (and interfacing systems), IA, CM, Records Manager (if a system of record), SW library.
 4. Notify/coordinate with Contracting, the COR, the support vendor(s).

8. <http://dcmo.defense.gov/publications/enterprise-transition-plan.html>

- 
5. Address interface impacts, and any dependent system vulnerabilities due to system retirement.
 6. Realign resources/modify contract support (programmer, system admin, help desk), software licenses.
 7. Complete the transition plan, if there is a replacement system.

8. <http://dcmo.defense.gov/publications/enterprise-transition-plan.html>

All current software should be documented by software name, company name, license number, date received, type data used, data sensitivity level

- **For old software that is no longer used or licensed, follow these guidelines to dispose of unused software:**
 - Destroy in accordance with (IAW) manufacturer end-user license agreements and local, state, and federal copyright law.
 - Destroy the information on the original disks or CDs. This is necessary to avoid having the old software removed from the garbage and used by an unlicensed party, thereby exposing the enterprise to copyright infringement.
 - Destroy the manuals according to sensitivity level.
 - Keep an inventory of serial numbers, dates of purchase, dates of destruction, and means of destruction. This will provide a complete audit trail in the event of a software audit.
- **If data will not be used in the replacement software, all sensitive data (e.g. Personally Identifiable Information(PII)) should be appropriately discarded by destroying the storage device IAW DOD hardware disposal procedures.**

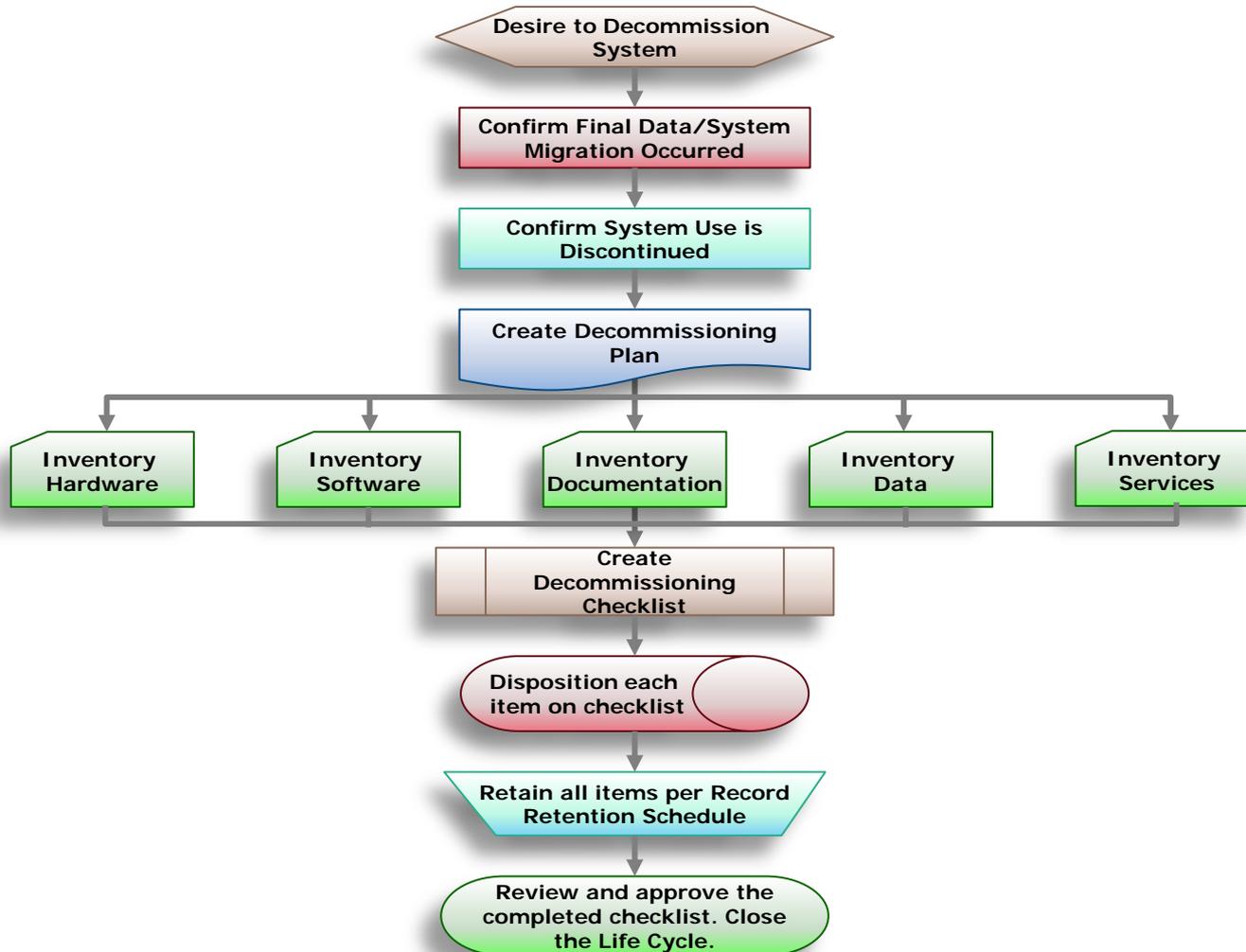
9. <http://www.softwaremetering.com/20030017.htm>

Solid State Devices: Use Caution



“Note about solid state devices: USB thumb drives, compact flash, MMC/SD, and the like are unreliable in the face of disk wiping protocols. Multi-pass wiping is not technically relevant for solid-state devices. More importantly, solid-state storage has a very limited number of read/write cycles and is designed with considerable surplus. This surplus storage is used to relocate data away from failing data segments. Wipe utilities cannot guarantee that all originally allocated blocks have been wiped. Further, they cannot insure new data is properly committed to the device. If disposal is the ultimate goal, physical destruction is strongly recommended.” ¹⁰

10. http://www.it.cornell.edu/security/depth/practices/media_destruct.cfm

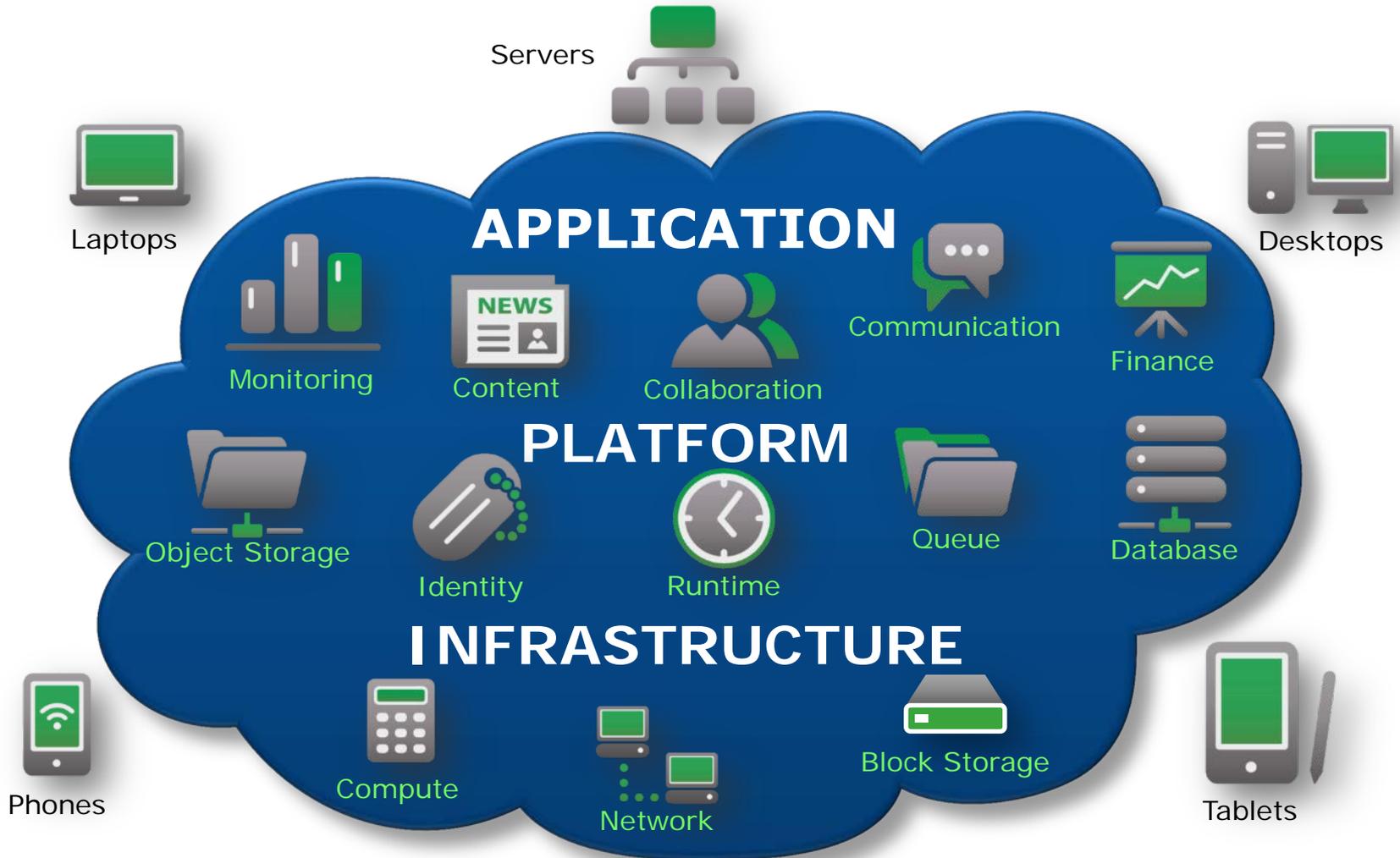


What is Cloud Computing? ¹²



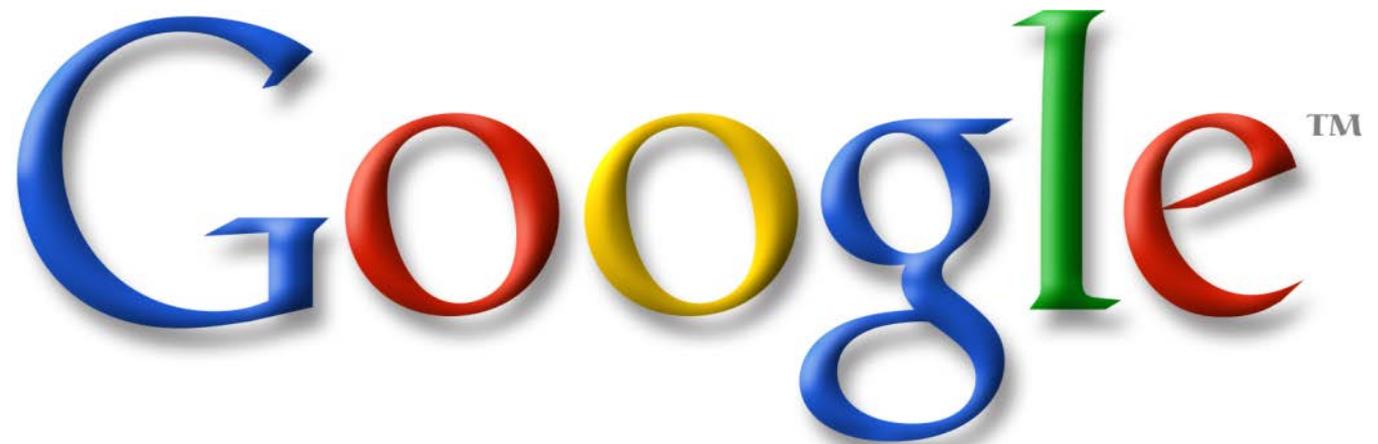
- **Cloud computing is very broadly defined as location-independent, ubiquitous computing and storage on demand.**
- **The National Institute of Standards and Technology (NIST) devotes an entire security publication (SP) to the definition.***
- **There are three major forms of cloud computing:**
 - **Pure infrastructure (infrastructure as a service, or IaaS)**
 - **A computing platform (platform as a service, or PaaS)**
 - **A fully supported application (software as a service, or SaaS)**

12. The NIST Definition of Cloud Computing, SP 800-145, Sept. 2011



Source: Unknown

“...you grant Google a worldwide, non-exclusive, royalty-free license to reproduce, adapt, modify, publish and distribute such Content on Google services for the purpose of displaying, distributing and promoting Google services.”¹³



Google™

13. <https://groups.google.com/forum/#!topic/google-groups-basics/2w9vibCbCes>

No liability for Deletion of Customer Data. The End-user agrees that, other than as described in these terms, O2 has no obligation to continue to hold, export or return the End User data. The End-User agrees that O2 has no liability whatsoever for deletion of the End-User Data pursuant to these terms. ¹⁴



14. <http://go.microsoft.com/?linkid=9708479>

Exit Strategy From Cloud Vendor

Because of the large amounts of data potentially involved, planning an exit strategy can help alleviate future problems. Termination provisions should be negotiated with the vendor at the beginning of the relationship.

Negotiation should include items such as:

- Causes for termination (e.g., convenience vs. breach)
- Lead time required for notifying the vendor of the desire to terminate the relationship ¹⁴

14. <http://go.microsoft.com/?linkid=9708479>

Exit Strategy From Cloud Vendor (Continued)

- The method to be used by the vendor to return any active data, as well as evidence and reports of completed disposition, to ensure a smooth and secure transition
- Other circumstances that could affect service (e.g., vendor is acquired, vendor experiences unexpected financial or staffing difficulties and can't provide the service you require, limitations on an organization's ability to change systems due to being "locked in" with a less flexible vendor) ¹⁴

14. <http://go.microsoft.com/?linkid=9708479>

Who Owns the Data

- Google or Amazon may have a legal responsibility to remove data from a server or client device under laws such as the Digital Millennium Copyright Act in the US.



Mitigating Cloud/Network Data Compromise



- **Hardware-asset management, which includes discovering unauthorized or unmanaged hardware on the agency's network.**
- **Software-asset management, to locate and identify unauthorized or unmanaged applications on the network.**
- **Managing trust in people granted access to the network, which focuses on the insider threat by looking for potential network abuses, such as deleting information or removing data that doesn't belong to them. ¹⁵**

15. <http://www.federalnewsradio.com/473/3164711/DHS-issues-6B-RFQ-for-continuous-monitoring-tools-services>

References

1. <http://computer.howstuffworks.com/cloud-computing/cloud-storage2.htm>
2. http://en.wikipedia.org/wiki/Systems_development_life-cycle
3. DoD Open Systems Architecture, Contract Guidebook for Program Managers v1.1, June 2013
4. ISO/IEC 9003:2004 Software Quality Management
5. Final Report of the Department of Defense and General Services Administration: Improving Cybersecurity and Resilience through Acquisition, June 2013
6. Department of Defense INSTRUCTION NUMBER 8510.01 November 28, 2007 ASD(NII)/DoD CIO
SUBJECT: DoD Information Assurance Certification and Accreditation Process
7. <http://www.archives.gov/about/laws/disposal-of-records.html>
8. <http://dcmo.defense.gov/publications/enterprise-transition-plan.html>
9. <http://www.softwaremetering.com/20030017.htm>
10. http://www.it.cornell.edu/security/depth/practices/media_destruct.cfm
11. Fasor Consulting, Decommissioning Rev. a 30 Apr 2003
12. The NIST Definition of Cloud Computing, SP 800-145, Sept. 2011
13. <https://groups.google.com/forum/#!topic/google-groups-basics/2w9vibCbCes>
14. <http://go.microsoft.com/?linkid=9708479>
15. <http://www.federalnewsradio.com/473/3164711/DHS-issues-6B-RFQ-for-continuous-monitoring-tools-services>

Related Articles ...

- <http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1>
- <http://www.gartner.com/technology/topics/cloud-computing.jsp>
- <http://www.softwaremetering.com/20030017.htm>
- <http://www.nextgov.com/mobile/2013/05/secret-service-explores-unified-system-manage-smartphones-tablets/63971/?oref=ng-dropdown>
- <http://www.fiercegovernmentit.com/story/nara-social-media-likely-record/2013-06-27>

Professor John F. Rice
Defense Acquisition University
7115 Old Madison Pike
Huntsville, AL 35758
256-922-8152
john.rice@dau.mil