

# Risk Management Framework Today

Formerly DIACAP Dimensions

... And Tomorrow



November 2011  
Issue 3, Volume 1

 Find us on  
Facebook



## In this issue:

Cloud Computing in the Federal Government	1
RMF and Contractors	1
Our Systems are getting Accredited!	3
Top Ten—Web Application Vulnerabilities	4
Training for Today ... and Tomorrow	5

## Cloud Computing in the Federal Government

By Kathryn Farrish

I am sure you've heard the phrase *cloud computing* (or one of its many variants) being tossed around the office, but do you really understand what it is, or how it benefits the IT industry? Cloud computing is the delivery of computing as a service, rather than a product, whereby shared resources, software and information are provided to computers and other devices as a utility over a network. In laymen's terms, it is a utility - similar to the idea of a customer receiving electricity in their own home. You have electricity in your house. You pay for it based on usage. You have no idea how it works, how it gets there, and that's okay. You don't need to. When a squirrel goes out on a power line and disrupts the service, you don't have to climb up a pole to fix it. Cloud computing works in the same manner.

Cloud computing can be immensely helpful to companies and organizations in that it provides benefits such as

reduced costs (capitol and operational), reliability, scalability, performance and maintenance. Because the hardware is not owned by the organization, and not housed within the organization, in-house IT support can be greatly reduced. Additionally, multiple users reduce costs by sharing resources. Rather than 100 organizations purchasing 100 separate humidity and temperature controls, in 100 separate data centers, the cost is divided by the number of tenants of the cloud service provider (CSP). Cloud computing also offers the benefit of scalability though the use of "on demand" provisioning of resources on a self-service basis in near real time. Reliability is improved because all products are provided remotely and, thus, creating redundancy at different locations is made easier.

The federal government is gradually understanding the capabilities and benefits of cloud computing and has created a draft program to implement it within the federal workspace. The

Cont. on page 4

## RMF and Contractors—"Does this stuff Apply to Me?"

We probably get several calls each week from companies asking if RMF (or FISMA or DIACAP) really applies to what they are doing. Unfortunately, there is considerable misunderstanding regarding the role of industry partners in these federally-mandated information system (IS) Certification and Accreditation (C&A) programs. We hope this article will help clarify things.

It is important to realize there are various types of relationships between

government agencies and private-sector contractors. Contractual details vary widely, but, generally speaking, most will fall into one of three general concepts of operations (CONOPS), which are as follows:

- **Direct Support Contractor.** In this CONOPS, a federal agency contracts with an industry partner to provide subject matter expert labor to support government-owned IS. Oftentimes, contractor employees will work directly at the federal site, although

Cont. on page 2

## Contractors and RMF

Cont. From page 1

work will sometimes take place at contractor offices. The IS being maintained belongs to the government and is typically housed in a government-owned data center.

- **IT-based Service Provider.** In this CONOPS, the contractor utilizes its own IS to process government data. This may or may not involve a direct link for data exchange between government and contractor data centers.
- **IT Product Developer.** In this CONOPS, the contractor manufactures a product (hardware, software, or both) for purchase or lease by the government. Such a product is intended for installation and operation within a government facility. Products sold to the government under this CONOPS are typically the same commercial off-the-shelf (COTS) products.

Direct support contractors will likely be called upon by their government customer to participate in the C&A process for the IS they are supporting. Specific assignments may include: scanning systems for compliance with Security Technical Implementation Guides (STIGs) or other configuration manuals; building and maintaining hardware/software inventories, network diagrams, and other “as built” documentation; developing and maintaining Standard Operating Procedures (SOPs); developing supporting documentation such as incident response plans, contingency plans, configuration management plans, etc.

IT-based Service Providers will need to work in partnership with their government customer to execute the C&A process for the IT infrastructure that

supports their mission. The contractor will need to ensure their systems and networks are configured in accordance with applicable security requirements, and that requisite documentation (policies, procedures, and “as built” documents) are in place. Contractor personnel with security responsibilities will need to meet the government’s requirements for training and certification. Additionally, the contractor must be prepared to support the government’s “independent validation” process, which may entail testing and observation by a government-designated reviewer.

IT Product Developers must first and foremost ensure that their product is capable of being installed and operated in accordance with applicable government security requirements. This effort may entail configuration changes to the product, and/or development of additional documentation describing how the product is to be operated in a secure environment. Depending on the specific contractual relationship with the government, the contractor may or may not be required to actively participate in the C&A process itself.

Regardless of a contractor’s specific relationship with the government, the following guidelines always apply:

DIACAP, FISMA and RMF are government-owned processes.

Contractors cannot independently seek certification of their systems or products. C&A must be done in “partnership” with a government customer, and only a duly authorized government representative can issue an accreditation.



## Our Systems are getting Accredited! Ugh!

By Betsy Taylor

I used to be a Unix Reviewer for DISA Field Security Operations (FSO). When we are talking about the Security Authorization (C&A) Process, FSO's role is that of the independent assessor/validator. Of course, they are one of many, but my job was to travel to government and contractor sites to assess the security of the Non-secure Internet Protocol Router Network (NIPRnet) and Secret Internet Protocol Router Network (SIPRnet). If your systems are on the Global Information Grid (GIG), you're fair game.

I went to some interesting sites, met a lot of great people, and worked with some very talented System Administrators (SA). I was an SA for many, many years, and I was visited by FSO on a couple of occasions to assess the security of the Unix systems for which I was in charge. It can be a nerve wracking experience, but it doesn't have to be. As a Reviewer, it was now my turn to work with those SA's that "used to be me". I tried very hard to put them at ease. After all, I wasn't there to test their skills or try my best to "fail" them. Of course, not all SA's are created equally, and each of them had a different point of view as to what this visit meant. Even the most seasoned SA's were nervous by my presence, for fear that I would find their systems to be full of CAT[egory] I and II findings. But rarely did I find that, because most SA's know that security is also their responsibility, and keeping up with patching and maintenance is an on-going process, not just something to do a week before the Assessment team arrives (ever heard of Continuous Monitoring?).

All visits began with an In-brief. Although almost all visits are scheduled

ahead of time (FSO does periodically perform "no notice" Cyber Command Readiness Inspections (CCRI's) at the direction of Cyber Command), the In-brief was a time to introduce the FSO team and site personnel, as well as apprising all parties as to the daily schedule of the visit during our [week-long, most of the time] stay. These In-briefs could be very telling. If upper management failed to relay the purpose of our visit to the SA's, the week began as a very tense one. That made both of our jobs harder.

The solution? Communication and education!! As a System Administrator, you play an important role in the C&A Process. It's all about managing risk on our network (the global network), and you have the day-to-day assignment of making sure that the systems you have been given the responsibility of securing is top notch. Make sure you know what's going on around you. Find out what is expected of you when an Assessor is coming for a visit. What will they want? Talk to your Information Assurance Manager/Officer (IAM/IAO). Educate yourself with the DoD Security Technical Implementation Guides (STIGs) and Checklists that DISA uses. Make sure you have procedures documented (because FSO *will* ask to see them).

The better educated and prepared you are, the better the site visit will be.



## IA Control Spotlight—Vulnerability Management

By Kathryn Farrish

The DoD Vulnerability Management Control protects against newly identified vulnerabilities in operating systems and software. The control requires that an organization have, in place, a documented Information Assurance Vulnerability Assessment (IAVA) process. The IAVA process begins with vulnerabilities being identified or reported to the DoD Information System Agency (DISA). The DISA DOD-Computer Emergency Response Team (DOD-CERT) researches the vulnerability and determines the impact, severity, and means of correcting or mitigating the risk associated with the vulnerability. If the results of this analysis indicate a need for action, the DoD-CERT will perform one of the following actions:

1. Issue an Information Assurance Vulnerability Alert (IAVA) - requires acknowledgement and compliance.
2. Issue an Information Assurance Vulnerability Bulletin (IAVB) - requires acknowledgement only.
3. Issue an Technical Advisory (TA) - Notification only.

Once the vulnerability notice has been developed, the DOD-CERT notifies the organizational point of contacts via approved channels that an alert, bulletin or technical advisory has been issued and that the details can be accessed at the DOD-CERT NIPERNET Web Page (<http://www.jtfgno.mil>)

The organizational Vulnerability Management Policy should include organizational processes that outline how official notifications of a vulnerability notice will be handled, who will implement them, and how the status of them will be tracked. Additionally, it should include the process used to

periodically scan servers with an approved vulnerability scanner. Approved vulnerability scanners can be found on the Common Criteria Portal (<http://www.commoncriteriaportal.org>). Some approved scanners include: Tenable Nessus, eEye Retina and McAfee).

All contracts for outsourced IT services should include requirements for an IAVA policy to be completed by the contractor, in accordance with the DoD 8500.2 requirements.

### Cloud Computing (Cont. from Page1)

Federal Risk and Authorization Management Program, or FedRAMP, has been established to provide a standard approach to Assessing and Authorizing (A&A) cloud computing services and products. The program provides a unified, government-wide risk management program focused on large, outsourced and multi-agency systems and it provides a standard approach to Assessing and Authorizing (A&A), formerly the C&A process. The program is managed by the General Services Administration (GSA), under the authority of the Federal CIO, and with interagency participation.

While FedRAMP is still in draft mode, GSA, the Defense Department and the Department of Homeland Security sent the final policy memo to OMB in September. They announced they are expecting an approval in November 2011 and will then publish official documents on how FedRAMP will work. Stay tuned to future issues of *RMF Today* as we will be following the unveiling of this worthwhile initiative!



## Top 10—Web Application Risks

By Kathryn Farrish

1. **Injection:** Examples include SQL, LDAP, HTTP header injection (cookies, requests) and OS command injections. Attacks occur when untrusted data, such as a query, command or argument, is sent to an interpreter. Vulnerable applications can be tricked into executing unintended commands or allowing the attacker to access, and modify data.

2. **Broken Authentication and Session Management:** Users are impersonated due to leaks or flaws in the authentication process. Attacks occur when a session ID is visible to others, timeouts are not properly set, SSL is not used, or any other flaw in the authentication scheme is detected.

3. **Cross Site Scripting (XSS):** XSS attacks occur when an application allows data that is not validated or escaped properly to be sent to a web browser. Malicious scripts are executed in the victim's browser allowing the attacker to hijack the user's session, steal cookies, deface websites, redirect users to malicious web sites and remote browser control.

4. **Insecure Direct Object References:** An attack occurs when an authorized user can change a parameter value that refers to a system object that they are not authorized for and includes almost any reference that can be reached by URL to include: references to files, paths, database keys, reflection by class name (e.g., JDBC connector class).

5. **Cross Site Request Forgery (CSRF):** Attacker creates malicious code to generate a forged request that the attacker tricks the victim into sending. Forged requests can be hidden in image tags, XSS attacks and a number of other

techniques. CSRF attacks can complete any transactions that the victim is permitted to perform such as access data, transfer funds or make purchases.

6. **Security Misconfiguration:** Attacker can exploit unsecured pages, default accounts, unpatched flaws or any other vulnerability that could have been addressed by proper system configuration. These attacks can result in a complete system compromise.

7. **Failure to restrict URL access:** This attack takes place when an authorized user can simply change a URL to access a privileged page. Attackers generally look for administrative functions to employ this attack on.

8. **Unvalidated Redirects and Forwards:** Unvalidated parameter allows an attacker to choose a destination page where they wish to send a victim to trick them into disclosing private information. Victims trust these links because the link is to a valid site.

9. **Insecure Cryptographic Storage:** The most common reason for this attack is that data that should be encrypted is stored in cleartext. It can result from the poor use of encryption algorithms or the continued use of proven weak algorithms. The use of weak or unsalted hashes to protect passwords is another common flaw that leads to this risk.

10. **Insufficient Transport Layer Protection:** Most commonly, this attack occurs when a site does not use SSL for pages that require authentication where an attacker can monitor network traffic to steal a users session cookie. Poorly configured SSL certificates can lull a user into accepting warnings for legitimate sites only to be tricked into accepting a phishing site's certificate.



1. *Injection*
2. *Broken Authentication and Session Management*
3. *Cross Site Scripting (XSS)*
4. *Insecure Direct Object References*
5. *Cross Site Request Forgery (CSRF)*
6. *Security Misconfiguration*
7. *Failure to restrict URL access*
8. *Unvalidated Redirects and Forwards*
9. *Insecure Cryptographic Storage*
10. *Insufficient Transport Layer Protection*

## Training for Today ... and Tomorrow

Since DoD is just at the early stages of its C&A transformation, we are continuing to offer our “traditional” DIACAP training program, which has recently been enhanced to include modules dedicated to the RMF transition.

Our FISMA RMF training program is suitable for Federal “civilian” agencies as well as DoD personnel looking for insight into the future of “C&A” within their programs.

Each of our training programs consists of a one-day Fundamentals class, followed by a three-day In Depth class. The cost of training is \$650 for the one-day class, \$1,500 for the three-day class, or \$1,935 for the full four-day program (both classes).



### Contact Us!

RMF Today ... and Tomorrow is a publication of BAI Information Security Consultants, Fairlawn, Virginia.

Phone: (540) 808-1050  
Fax: (540) 808-1051  
Email: [RMF@RMF.ORG](mailto:RMF@RMF.ORG)

DIACAP Fundamentals (One-day)	DIACAP In-Depth (Three-day)
5 Dec 2011 (NCR)	6-8 Dec 2011 (NCR)
13 Feb 2012 (NCR)	14-16 Feb 2012 (NCR)
27 Feb 2012 (H)	28 Feb-1 Mar 2012 (H)
12 Mar 2012 (CS)	13-15 Mar 2012 (CS)
23 Apr 2012 (NCR)	24-26 Apr 2012 (NCR)
4 June 2012 (H)	5-7 June 2012 (H)
18 June 2012 (CS)	19-21 June 2012 (CS)

FISMA RMF Fundamentals (One-Day)	FISMA RMF In-Depth (Three-Day)
30 Jan 2012 (DC)	31 Jan-2 Feb 2012 (DC)
26 Mar 2012 (DC)	27-29 Mar 2012 (DC)
16 Apr 2012 (H)	17-19 Apr 2012 (H)
30 Apr 2012 (CS)	1-3 May 2012 (CS)
21 May 2012 (DC)	22-24 May 2012 (DC)

(H) - Huntsville, AL, (CS) - Colorado Springs, CO,  
(NCR) - Ashburn, VA, (SD) - San Diego, CA,  
(A) - Anaheim, CA, (DC) - Washington DC

On-line registration and payment for all scheduled classes is available at [www.diacap.net](http://www.diacap.net) (for DIACAP classes) or [www.fisma1.net](http://www.fisma1.net) (for FISMA RMF classes). Registration can also be done by downloading a registration form and submitting the completed form by FAX or email.

Payment arrangements include credit cards, SF182 forms, or purchase orders.

Please visit [www.diacap.net](http://www.diacap.net) or [www.fisma1.net](http://www.fisma1.net) for the latest training schedule, including any new dates or locations.

For Customers in other locations or those with specific scheduling requirements,

we offer the option of “on-site” training. All you need is a group of students (at least 8-10) and a suitable classroom facility. We offer a substantial discount over the normal “per student” registration cost; the discount grows larger as the class size increases. Our “on-site” training fee includes all instructional services, training materials, and instructor travel expenses. Most importantly, you will avoid the travel expenses associated with sending your people to training away from the office. Please contact us to request an on-site training quotation.