Peeling Back the Onion: Drupal Security and Compliance
Who are we...
CivicActions is ...

Open
Agile
Transparent
What is security?
WHAT ARE THE GOALS OF SECURITY?

Problem of Security
Security Objective: Practical, preventative measures for mitigating risk
COMPLIANCE DOES NOT MEAN SECURITY

Goals of Security

Information Assurance

Image courtesy of the book:

*Information Security Principles of Success*
Breithaupt and Merkow, 2014
WHAT ARE THE GOALS OF SECURITY?

The practice changes for each system and need
Let’s evaluate some guiding principles to achieve the outlined goals
COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation
COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation
Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation
Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation
Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation
Be proactive and test your security practices
Why Compliance?
Compliance is not just a good idea, it’s the law
Compliance is not just a good idea, it’s the law.
When you’re told that the new system has to be compliant
The Risk Management Framework

Continuous Monitoring is to be implemented by 2017 per OMB M-14-03.

See also: CDM from DHS and GSA.
Control Types

● Administrative
  ○ Guidelines, procedures (Security Policy)

● Technical
  ○ Intrusion detection systems, ACLs (Least Privilege)

● Physical
  ○ Physical (USB, media) access (Separation of Duties)
Practical Benefits of Compliance

- Scanning regularly (CVEs, STIGs, …)
- Keeping LAMP stack up-to-date
- Keeping Drupal up-to-date
- Reviewing logs
- Managing Access Control
- Incident Response Training
- Bastion SSH host and CDN
Compliance does not mean Security
Compliance controls provide guidance, but they do not prescribe security practices.

How are they related?
COMPLIANCE DOES NOT MEAN SECURITY

CONFUSION

CONFUSION EVERYWHERE...
COMPLIANCE DOES NOT MEAN SECURITY

1. Network - Ports, VPC, Monitor
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
3. Application - Drupal, Solr, HTTPD, JavaScript
4. Data - MySQL, Shared Filesystem
COMPLIANCE DOES NOT MEAN SECURITY

1. Network - Ports, VPC, Monitor
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
3. Application - Drupal, Solr, HTTPD, JavaScript
4. Data - MySQL, Shared Filesystem
1. Network - Ports, VPC, Monitor
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
3. Application - Drupal, Solr, HTTPD, JavaScript
4. Data - MySQL, Shared Filesystem

COMPLIANCE DOES NOT MEAN SECURITY
COMPLIANCE DOES NOT MEAN SECURITY

1. Network - Ports, VPC, Monitor
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
3. Application - Drupal, Solr, HTTPD, JavaScript
4. Data - MySQL, Shared Filesystem
Look at each tier of the system to map controls to security practices
COMPLIANCE DOES NOT MEAN SECURITY

Making the onion tasty
What are the most common compliance controls you need to be aware of?
Typical Controls

- AC: Access Control
- IA: Identification and Authentication
- AU: Audit & Accountability
- CM: Configuration Management
- RA: Risk Assessment
The 18 RMF (Risk Management Framework) “Control Families”

Defined in NIST SP 800-37 Rev 4

<table>
<thead>
<tr>
<th>Families</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC - Access Control</td>
</tr>
<tr>
<td>AU - Audit and Accountability</td>
</tr>
<tr>
<td>AT - Awareness and Training</td>
</tr>
<tr>
<td>CM - Configuration Management</td>
</tr>
<tr>
<td>CP - Contingency Planning</td>
</tr>
<tr>
<td>IA - Identification and Authentication</td>
</tr>
<tr>
<td>IR - Incident Response</td>
</tr>
<tr>
<td>MA - Maintenance</td>
</tr>
<tr>
<td>MP - Media Protection</td>
</tr>
<tr>
<td>PS - Personnel Security</td>
</tr>
<tr>
<td>PE - Physical and Environmental Protection</td>
</tr>
<tr>
<td>PL - Planning</td>
</tr>
<tr>
<td>PM - Program Management</td>
</tr>
<tr>
<td>RA - Risk Assessment</td>
</tr>
<tr>
<td>CA - Security Assessment and Authorization</td>
</tr>
<tr>
<td>SC - System and Communications Protection</td>
</tr>
<tr>
<td>SI - System and Information Integrity</td>
</tr>
<tr>
<td>SA - System and Services Acquisition</td>
</tr>
</tbody>
</table>
What is an example?
AC: Access Control

- AC-2 Account Management
- AC-2(5) Inactivity Logout
- AC-5 Separation of Duties
- AC-6 Least Privilege
- IA-5 Authenticator Management
AC: Drupal Solutions

- Roles and Perms
- Autologout
- Password Policy
- TFA / SimpleSAMLPHP
- * Permissions (Field Permissions, Taxonomy Access Control, etc)
Handout

We have a handout that outlines additional security and compliance recommendations.
Current Challenges
1. Poorly defined best practices
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
4. Tools are not accessible
5. No magic bullet (security is relative to your system)
CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
4. Tools are not accessible
5. No magic bullet (security is relative to your system)
CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
3. **Tools are not robust or comprehensive**
4. Tools are not accessible
5. No magic bullet (security is relative to your system)
CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
4. **Tools are not accessible**
5. No magic bullet (security is relative to your system)
CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
4. Tools are not accessible
5. No magic bullet (security is relative to your system)
Fun Stuff
Where do we see security and compliance going?

COMPLIANCE DOES NOT MEAN SECURITY
Innovation at every tier of the onion

COMPLIANCE DOES NOT MEAN SECURITY
The three year ATO cycle is transforming into continuous assurance
COMPLIANCE DOES NOT MEAN SECURITY

Compliance is pushing more into DevOps
COMPLIANCE DOES NOT MEAN SECURITY

Build small, discrete components and automate
Intrusion Detection
Isolate Threats
Minimize Damage

COMPLIANCE DOES NOT MEAN SECURITY
System predicts 85 percent of cyber-attacks using input from human experts

Examples
OpenSCAP is free and open source, automated security scanning for operating systems* and selected applications.

*only Red Hat 6 & 7 for now, but can be extended
COMPLIANCE DOES NOT MEAN SECURITY

A YAML-Powered Antidote To Bureaucracy
It's a powerfully simple idea.
It's a schema.
It's a set of tools and best practices.
It's a community.

A YAML-Powered Antidote To Bureaucracy

It's a powerfully simple idea.
To improve the quality of our software development, we use continuous integration. To improve the reliability of our deployment, we use continuous delivery. To improve the security of our systems, we can use continuous authorization.

Simply put, the tools that we use to develop and operate software, should also be used to generate and validate assessment and authorization packages.

Every commit runs the tests. Every passing build, updates the system security plan. Every deployment includes updates to continuous monitoring.

Software as Code.
Tests as Code.
Infrastructure as Code.
Compliance as Code.

It's a schema.
By adopting a standard approach to documenting "controls" (whether Technical, Operational, or Management) we can rapidly build a community of vendors and operators. You can see the current (and evolving) OpenControl schema here.
COMPLIANCE DOES NOT MEAN SECURITY

Component Schema
Here is an example component schema:

```
# CloudFoundry-UAA.yaml
---
name: User Account and Authentication (UAA) Server
references:
- name: User Account and Authentication (UAA) Server
  url: http://docs.pivotal.io/pivotalcf/concepts/architecture/uaa.html
governors:
- name: Cloud Foundry Roles
satisfies:
  NIST-800-53:
  AC-2: Cloud Foundry accounts are managed through the User Account and Authentication (UAA) Server.
```

You can find the complete file on github.
The GovReady Dashboard puts compliance info in a Drupal report.

*Alpha - Not yet ready for production, but interesting work.
Call To Action
We need to define best practices and build the tools to support it.
COMPLIANCE DOES NOT MEAN SECURITY

COMPLIANCE DOES NOT MEAN SECURITY

ansible-role-govready

Role to install GovReady.
GovReady is a super easy to use commandline toolkit for running security scans on open source servers and software. Technically, GovReady is a bash wrapper around OpenSCAP, a NIST certified SCAP toolkit.
GovReady depends upon: - OpenSCAP role must be installed on all instances - SCAP Security Guide role must be installed on the GovReady "dashboard" instance.
COMPLIANCE DOES NOT MEAN SECURITY

Drupal 8 Security Review
New Plugin System
Code Sprint
Thank you.