The State of Compliance Frameworks and compliance maturity
What’s a framework?
What do we know we have to do?

1. Review each authority document.
2. Determine the IT control requirements specific to that document.
3. Determine if those controls are in-scope for their organization and the information they manage.
4. Implement the appropriate in-scope controls.
5. Conduct a series of audits to ensure the organization’s compliance level.

Frameworks provide assistance for this process by creating a set of controls that can (hopefully) encompass or at least accommodate the various regulatory statutes that crop up. In so doing, the statute can then be compared to the framework and where the two match, the organization following the framework can attest that they have put into place controls that meet those found in the statute.
A framework is an extensible structure for describing a set of concepts, methods, and technologies as an integrated set of policies and procedures designed to assist management to achieve its goals and objectives.
The major frameworks usable by IT

- AICPA/CICA Trust Services, Principles, and Criteria
- Carnegie Mellon University Software Engineering Institute (CMU/SEI) OCTAVE
- CICA CoCo – Criteria of Control Framework
- CICA IT Control Guidelines
- CMMI – Capability Maturity Model Integration
- CobiT – Control Objectives for Information and related Technology
- COSO – Internal Control Integrated Framework
- GAISP – Generally Accepted Information Security Principles
- ISF Standard of Good Practice for Information Security
- ISO 17799:2005
- ISO 9000
- ITIL – the IT Infrastructure Library
- Malcolm Baldridge National Quality Program
- Organization for Economic Cooperation and Development (OECD) Principles of Corporate Governance
- OPMMM – Organizational Project Management Maturity Model
- Six Sigma
- Recommended Security Controls for Federal Information Systems, NIST SP 800-53
- The FFIEC Information Technology Examination Handbook series
This is very inefficient!

Legal authority

Popular opinion

Organizational decree

Regulations

Standards

Policies & procedures

Public

Reg A

Reg B

Reg C
This is very inefficient!
What are the core elements that *must* be unified?
Metadata is definitional data that provides information about, or documentation of, other data managed within an environment.

Learning to properly track authority documents, we had to define the

- data elements,
- the structures of those elements, and
- descriptive information about the context, quality, or condition of those elements
The list authority documents

- http://www.unifiedcompliance.com/free-ad-list.html
Controlled vocabulary

- A controlled vocabulary is a collection of preferred terms that are used to assist in more precise retrieval of content.

- By harmonizing the terms that different authority documents use for the same type of information, controls, activities, etc., we can more precisely define when controls overlap and when they don’t.
  - ePHI
  - PIN
  - Cardholder data
  - SSNs
  - Restricted data
Control descriptions
Defining and abstracting controls

- **Definition**: To control is an activity conducted to bring into check (to manage or to verify), or to constrain (to restrict or confine) something, the results of which bring forth a demonstrable outcome. [de facto]

- **Abstraction**: Each control can be broken down into two parts,
  - the action with the demonstrable outcome being called for and
  - the parameters associated with the action

The risk assessment process is conducted in two steps. The first step defines the boundary of the environment, determines the scope of the assessment and selects the appropriate methodology to use. In step two the risk analysis is conducted. The risk analysis can be broken down into asset identification, threat and vulnerability identification, likelihood assessment, and risk measure... The Reference and Further Reading Sections of this document provide some information on LAN threats and vulnerabilities.
Ontology

- Ontologies are a rich, controlled hierarchical order of semantic relationships
- We must build out a hierarchical structure of compliance controls based upon the relationships defined in the control activities and demonstrable outcomes

- Define the scope of the organizational compliance framework and controls for your organization [Implied]
  - Define external rules that govern information systems, information, and information technology [Implied]
    - Maintain full documentation of all policies, standards, and procedures that support the compliance effort
Maintain full documentation of all policies, standards, and procedures that support the compliance effort.

- Which assets are in scope?
- To whom should this be assigned?
- What metrics should be applied?
- What policy or standard should this be assigned to?
- How should this be audited?
And it has to accommodate all authority documents

100s

And

100s
The UCF’s public XML structures provide all three
Beyond the Handshake Between Auditors and CMMI®

A Look Into Auditing for Process Maturity
<table>
<thead>
<tr>
<th>Step 1</th>
<th>Business Acceptance</th>
<th>Plan</th>
<th>Implementation</th>
<th>Communicating with feedback</th>
<th>Optimizing</th>
<th>Compliance and CMMI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
"By 2010, up to 15% of large enterprises will continue to lag in a blissful ignorance state of compliance program maturity, while about 20% will reach a state of operations excellence" (Gartner analyst French Caldwell)
Obvious discrepancies

- There are 2407 unique controls identified to date
- There are 695 matching audit questions to date
- Not one of those audit questions asks about the maturity of the compliance process or provides a methodology for rating the maturity of the process
Awareness auditing

- There are several audit questions pertaining to compliance awareness, security awareness, etc.
- 99% of auditors do not audit for awareness process improvement.
- Even though there is a very specific audit question asking for the full list of authority documents that must be followed, no auditors audit for the presence of a full list of authority documents that must be followed.
<table>
<thead>
<tr>
<th>ID</th>
<th>Common Name</th>
<th>URL</th>
<th>Type</th>
</tr>
</thead>
</table>

**Facilities**

These are all the resources to house and support information systems. A physical location containing the equipment, supplies, communication lines (voice and data), and related data to perform transactions required under normal operating conditions. See also computer facility. [Cobit, Centers for Medicare & Medicaid Services (CMS), ISO/IEC 27001:2005]

**Facsimile (FAX)**

A process of transmitting documents by scanning them to digital, converting to analog, transmitting over phone lines and reversing the process at the other end and printing. [Section 4001]

**Fail safe**

Automatic protection of programs and/or processing systems when hardware or software failure is detected. [US National Information Assurance (IA) Glossary]

**Fail soft**

Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent. [US National Information Assurance (IA) Glossary]
<table>
<thead>
<tr>
<th>Citation</th>
<th>Control title</th>
<th>Control guidance</th>
<th>Control hierarchy</th>
<th>ID</th>
<th>Policy statement</th>
<th>Authority document guidance</th>
<th>Audit guidance</th>
<th>Metric guidance</th>
<th>Taxonomy</th>
<th>Date Added</th>
<th>Date Modified</th>
</tr>
</thead>
</table>

**Harmonized control lists**

**Unified Compliance Framework**

<table>
<thead>
<tr>
<th>Control Title</th>
<th>ID</th>
<th>Policy</th>
<th>Authority</th>
<th>Audit</th>
<th>Metric</th>
<th>Taxonomy</th>
<th>Date Added</th>
<th>Date Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payment Card Industry Implied</td>
<td>C</td>
<td>✓</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**ID Policy statement**

- Authority document guidance
- Audit guidance
- Metric guidance
- Taxonomy
- Date Added
- Date Modified
ISACA and the IIA have huge quantities of documentation calling for a RACI assignment scheme.

- **Not one** audit question calls for a RACI style audit of assignment.
- Only **ten** audit questions require testing or examining for the assignment of responsibility.
This area is fully baked

All of the audit questions surrounding policies and procedures ask to examine them as a part of the organization’s compliance process.

None of the audit questions ask to link policies to control lists.

All of the questions seem to assume the managed level of maturity.

GRC tools are now moving organizations directly into the automation of the managed level and toward the optimizing level.

---

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Acceptance</td>
<td>Responsibility Accountability</td>
<td>Policies and Procedures</td>
<td>Skills &amp; Training</td>
<td>Tools &amp; Automation</td>
<td>Measurement and Metrics</td>
</tr>
</tbody>
</table>
Ontologically-based policies

Step 1

Policies and Procedures

Step 2

Awareness and Acceptance

Step 3

Responsibility Accountability

Step 4

Skills & Training

Step 5

Tools & Automation

Step 6

Measurement and Metrics
### Ontologically-based policies

<table>
<thead>
<tr>
<th>ID</th>
<th>Policy statement</th>
<th>Authority document guidance</th>
<th>Audit guidance</th>
<th>Metric guidance</th>
<th>Taxonomy</th>
<th>Date Added</th>
<th>Date Modified</th>
</tr>
</thead>
</table>

**Step 1**
- Awareness and Acceptance

**Step 2**
- Responsibility and Accountability

**Step 3**
- Policies and Procedures

**Step 4**
- Skills & Training

**Step 5**
- Tools & Automation

**Step 6**
- Measurement and Metrics

---

#### Common Name
- URL
- Type
- Description
- Cost
- Date Added

---

The organization will ensure that PKI authentication security issues, updates, and unlock keys, provide for expiration of keys, ensure valid certificates, update the list of revoked certificates, and log the use of the root key.  

The organization will maintain access to cryptographic keys to the lowest number of custodians necessary.  

The organization will store cryptographic keys securely in the fewest possible locations and forms.  

The organization will ensure that keys are changed periodically to ensure that they have not been compromised.  

The organization will promptly destroy all cryptographic keys once their retention period has ended, ensuring that the destruction has been properly documented.  

The organization will ensure that it requires 2 or 3 people, to control cryptographic keys, each knowing only their own part.  

The organization will prevent the unauthorized substitution of cryptographic keys.  

The organization will immediately replace, and document any suspected or compromised keys.  

The organization will immediately revoke old or invalid keys.  

The organization will require each cryptographic key custodian to sign a form stating that they both understand and accept the organization's key custodian policies and their key custodian responsibilities.  

The organization will use strong cryptography and encryption techniques such as SSL, FTP, and IPSec to safeguard confidential data during transmission over public networks.  

The organization will ensure that all confidential information is prohibited from being sent using either instant messaging or e-mail.  

The organization will provide transaction authorization.  

The organization will ensure non-repudiation.  

The organization will ensure that all systems transmitting confidential information across public networks or wireless networks amongst the transmissions using such techniques as VPNs, WPA for wireless, or SSL at 128-bit.  

b. Supporting documents
Ontologically-based policies

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Citation
Control title
Control guidance
Control hierarchy

ID
Policy statement
Audit question
Authority
document guidance
Audit guidance
Metric guidance
---
Taxonomy
Date Added
Date Modified

Common Name
URL
Type
Description
---
Cost
Date Added
Skills and training

- Only those controls focused on training have a direct correlation.
- All of the audit questions surrounding controls that address training have direct training process questions associated with them.
- None of the rest of the audit questions even ask if those assigned are properly training to carry out their assignments.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Acceptance</td>
<td>Responsibility Accountability</td>
<td>Policies and Procedures</td>
<td>Skills &amp; Training</td>
<td>Tools &amp; Automation</td>
<td>Measurement and Metrics</td>
</tr>
</tbody>
</table>
Not much is happening…
Tools and automation

- Only those controls focused on tools have a direct correlation
- All of the audit questions surrounding controls that address tools or automation have direct tools or automation process questions associated with them
- Only those audit questions surrounding configuration have any tools and automation process questions baked in
- Tools, such as NetIQ’s AEGIS, will possibly be the future of automation and will therefore force the issue

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Acceptance</td>
<td>Responsibility Accountability</td>
<td>Policies and Procedures</td>
<td>Skills &amp; Training</td>
<td>Tools &amp; Automation</td>
<td>Measurement and Metrics</td>
</tr>
</tbody>
</table>
Process automation XML
1. Initiate policy scan
   Or scan on an existing schedule

2. Identify resulting policy violations
   Send an event to Aegis, triggering a process

3. Aegis notifies stakeholder of policy violations via email, ticket, etc.

4. Stakeholder clicks on link to Aegis Web Console

5. Stakeholder chooses pre-defined response based on policy
   a) Create exceptions for violations
   b) Request remediation via a change request

6. Stakeholder selects remediation level
   a) Overall template level
   b) Individual check level
   c) Individual data element

7. Aegis notifies security team of requested exceptions

8. Security team approves exceptions
   All or selectively

9. Aegis puts exceptions in place in SCM

10. Optional – re-run scan to validate final results and go back to step 2 if necessary

Closed loop exception management
Closed loop vulnerability remediation

1. Initiate vulnerability & policy violation scan
   Or scan on an existing schedule

2. Identify resulting vulnerabilities or policy violations

3. Request permission to remediate via existing Change Management process (RFC)
   Group by machine, service, vulnerability class, compliance mandate, etc.

4. Monitor for approved RFC

5. Initiate remediation
   Using provisioning tools or by assigned administrator

6. Initiate scan to verify remediation
   Verify that violation was indeed remediated

7. Perform system health check
   After change, verify that remediation did not impact service levels

8. Relate changes to impacts
   Search other tools for downstream impacts from change such as performance problems, new policy violations, etc.

9. Close change request
   Or escalate if impacts are found
**Defined metrics linked to defined controls**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Acceptance</td>
<td>Responsibility and Accountability</td>
<td>Policies and Procedures</td>
<td>Skills &amp; Training</td>
<td>Tools &amp; Automation</td>
<td>Measurement and Metrics</td>
</tr>
</tbody>
</table>

**Policies and Procedures**

- Defined metrics linked to defined controls
- Key IT Assets for which an Assurance Strategy Has Been Implemented

**Citation**

- Policy statement
- Audit question
- Authority document guidance
- Audit guidance
- Metric guidance
- Taxonomy

**ID**

- Policy statement
- Audit question
- Authority document guidance
- Audit guidance
- Metric guidance
- Taxonomy

**Control title**

- Citation
- Control title
- Control guidance
- Control hierarchy

**Control guidance**

- ID
- Policy statement
- Audit question
- Authority document guidance
- Audit guidance
- Metric guidance
- Taxonomy

**Control hierarchy**

- Citation
- Control title
- Control guidance
- Control hierarchy

**Common Name**

- URL

**Type**

- Description

**Cost**

- Date Added

**Publication date**

- Common Name
- URL
- Type
- Description
- Cost
- Date Added
Measurement and metrics

- Auditors require
  - 96% formal metrics policy
  - 88% formal metrics reporting standard
  - 100% governance metrics
  - 88% management metrics
  - 93% technical metrics

- Organizations have
  - 58% formal metrics policy
  - 50% formal metrics reporting standard
  - 50% governance metrics
  - 47% management metrics
  - 50% technical metrics

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
<th>Step 5</th>
<th>Step 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awareness and Acceptance</td>
<td>Responsibility Accountability</td>
<td>Policies and Procedures</td>
<td>Skills &amp; Training</td>
<td>Tools &amp; Automation</td>
<td>Measurement and Metrics</td>
</tr>
</tbody>
</table>