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.

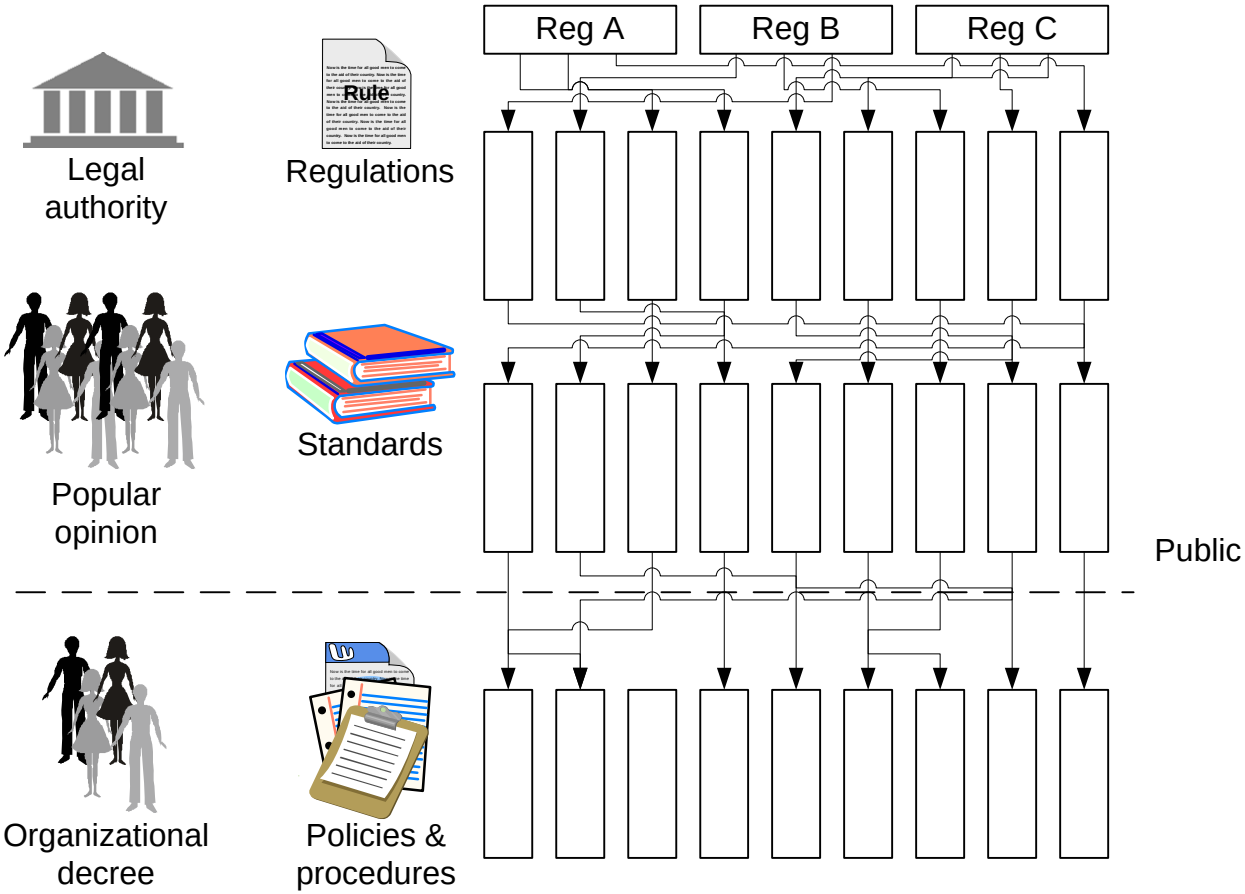
Framework definition

- 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
- **Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**
- **Recommended Security Controls for Federal Information Systems, NIST SP 800-53**
- **The FFIEC Information Technology Examination Handbook series**

This is *very* inefficient!

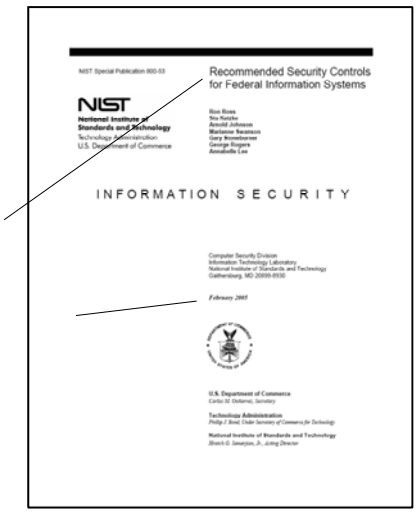


This is *very* inefficient!

What are the core elements that *must* be unified?

Authority Documents

Authority Documents



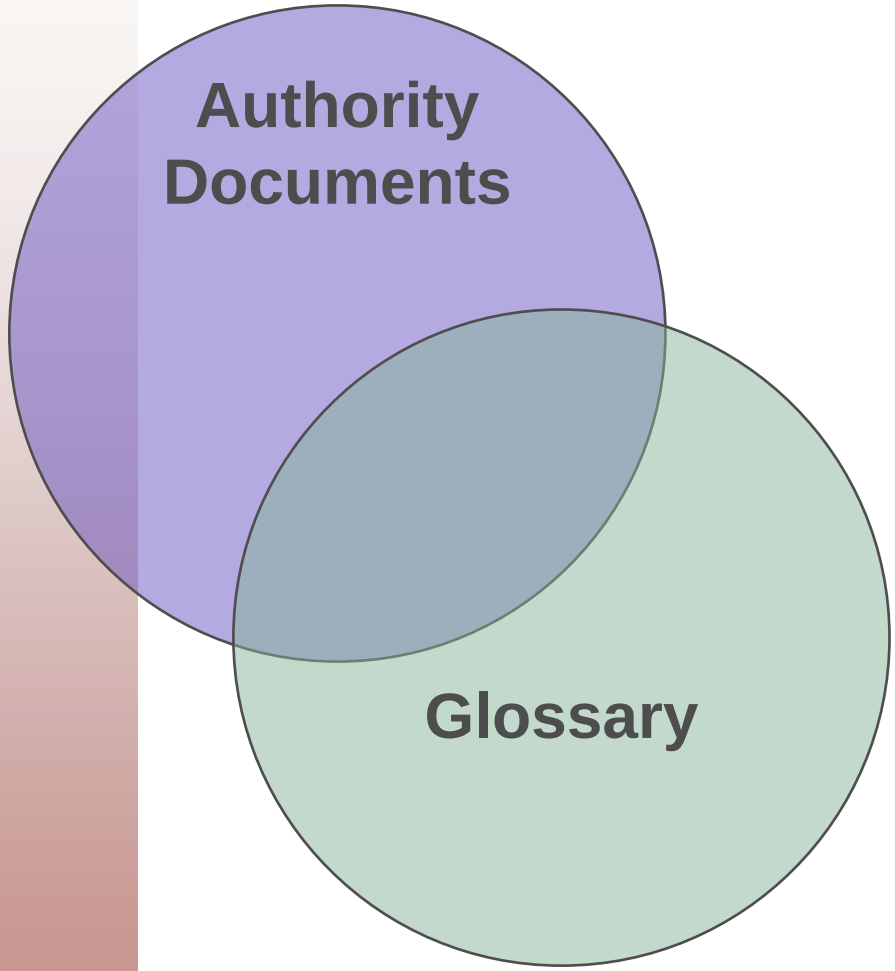
Metadata

- 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

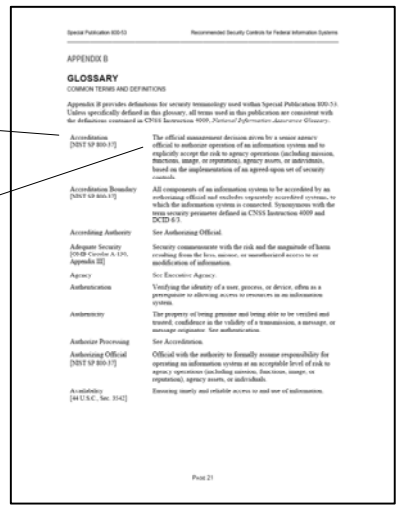
- http://www.unifiedcompliance.com/free-ad-list.html

Terms



Term

Definition



Special Publication 800-53 Recommended Security Controls for Federal Information Systems

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation [NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST GD 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorize Processing	See Accreditation.
Authorizing Official [NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.

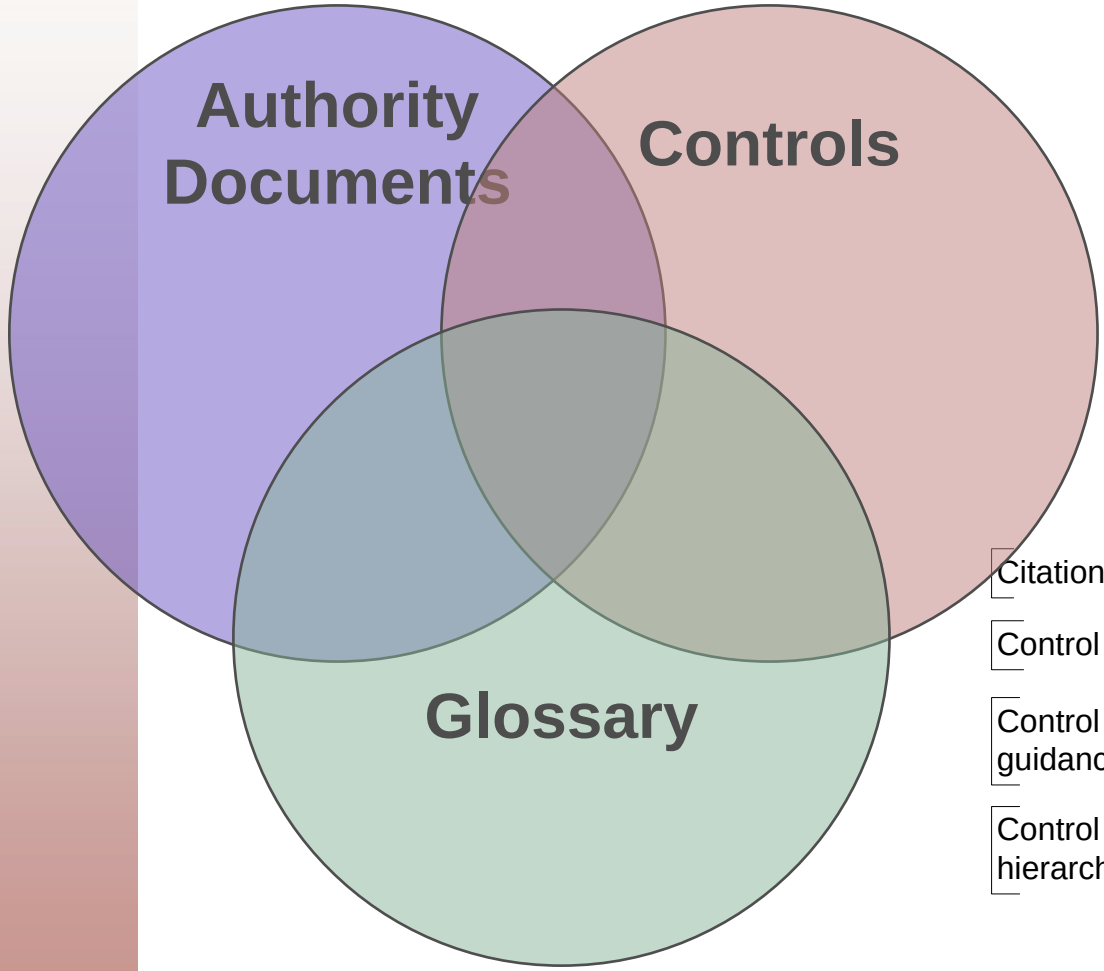
Page 21

ID
Acronym
Harmonized definition
References to other authority documents
--
Taxonomy
Date Added
Date Modified

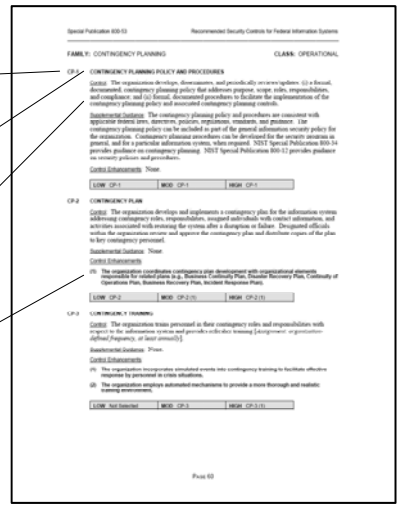
Controlled vocabulary

- 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



- Citation
- Control title
- Control guidance
- Control hierarchy

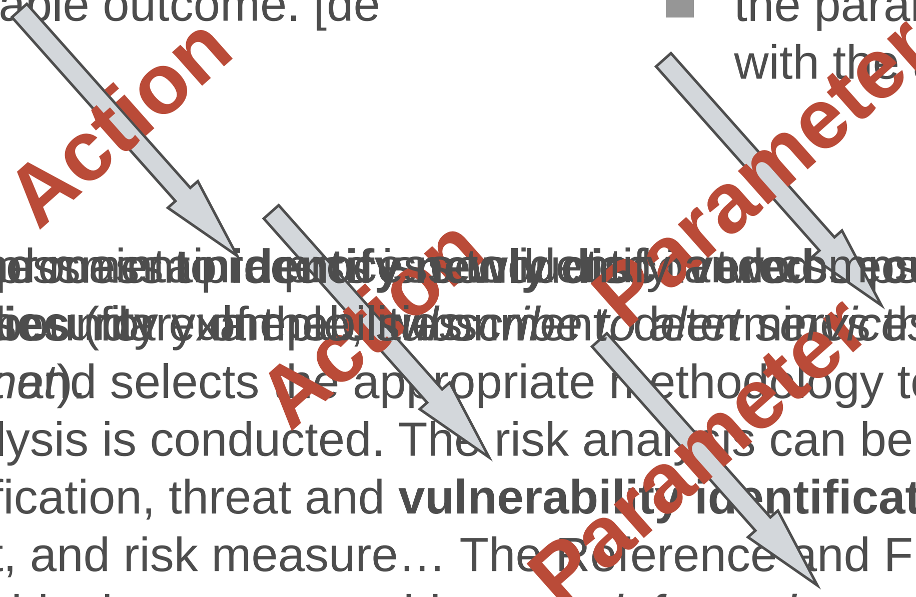


ID
Policy statement
Audit question
Authority document guidance
Audit guidance
Metric guidance
--
Taxonomy
Date Added
Date Modified

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



Establish and maintain procedures to **identify new security vulnerabilities** (for example, *subscribe to alert services freely available on the Internet*).

Risk assessment [illegible] The first step 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*.

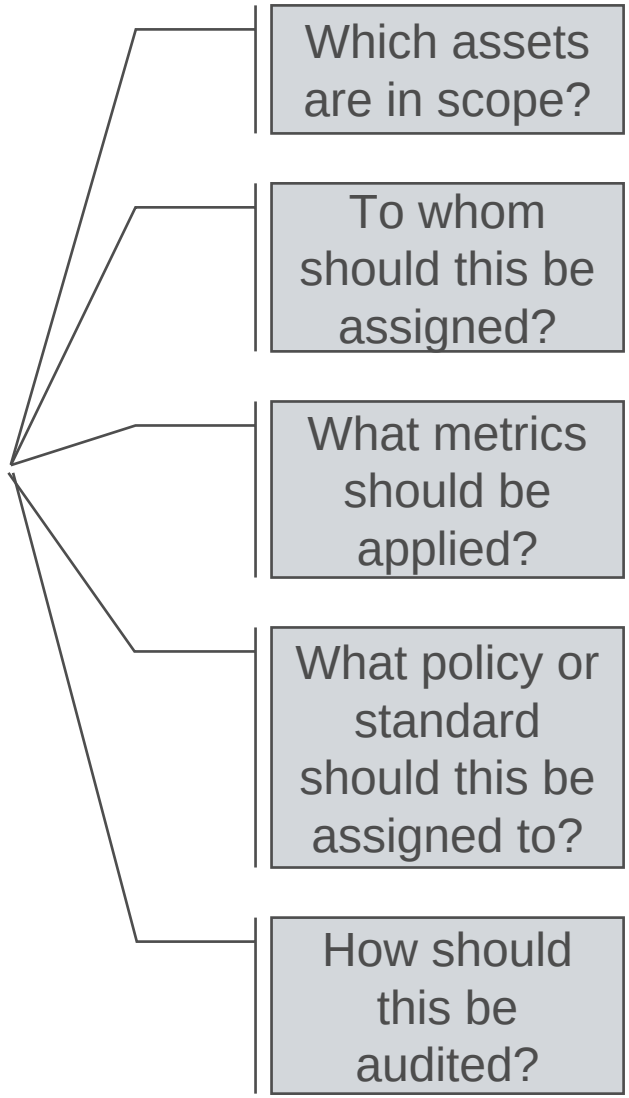
Ontology

- 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

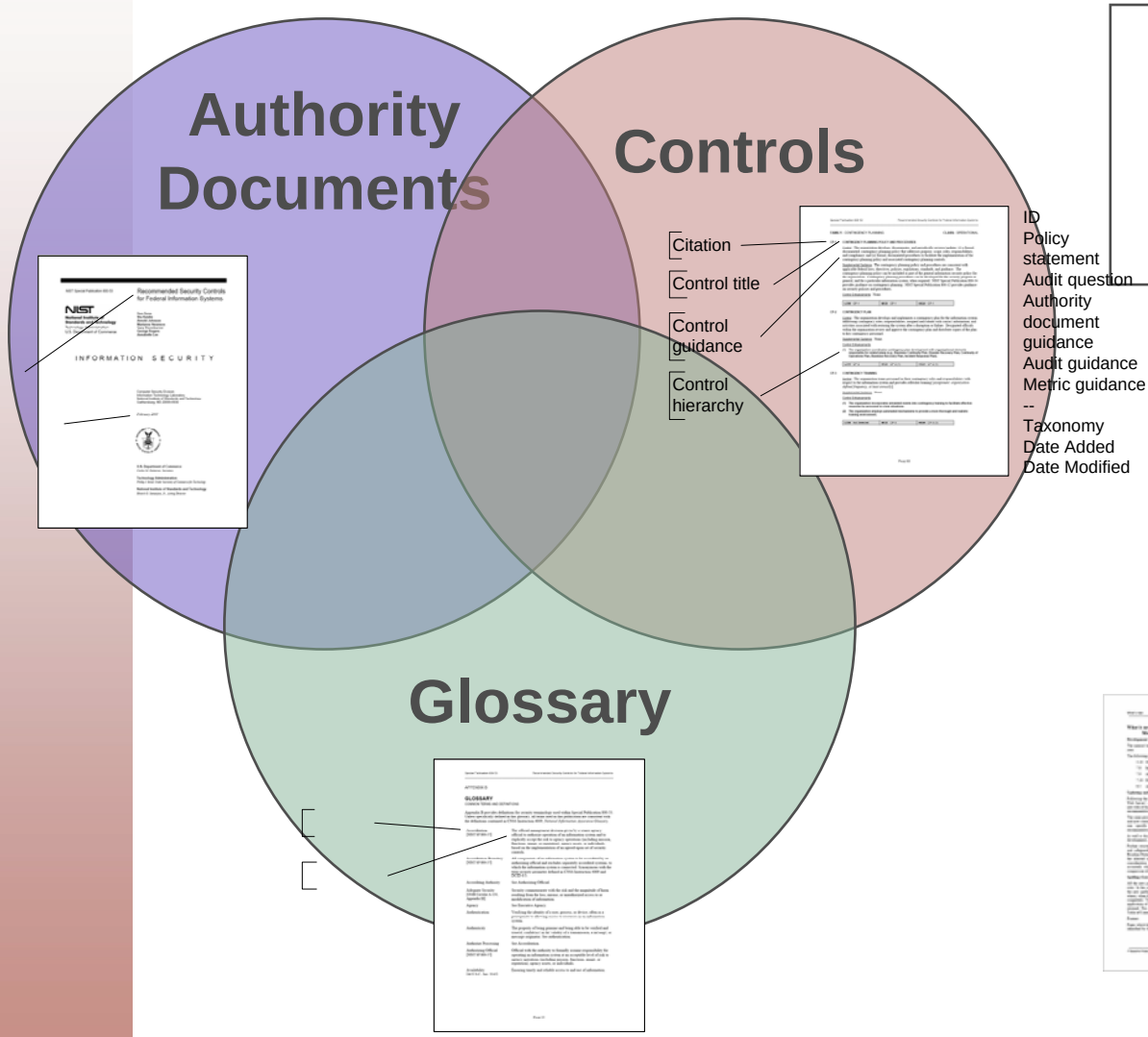
- Define the scope of the organizational compliance framework and controls for your organization [Implied]
  - Define external rules that govern information systems, information, and information technology [Implied]
    - Maintain full documentation of all policies, standards, and procedures that support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

Control scoping metadata

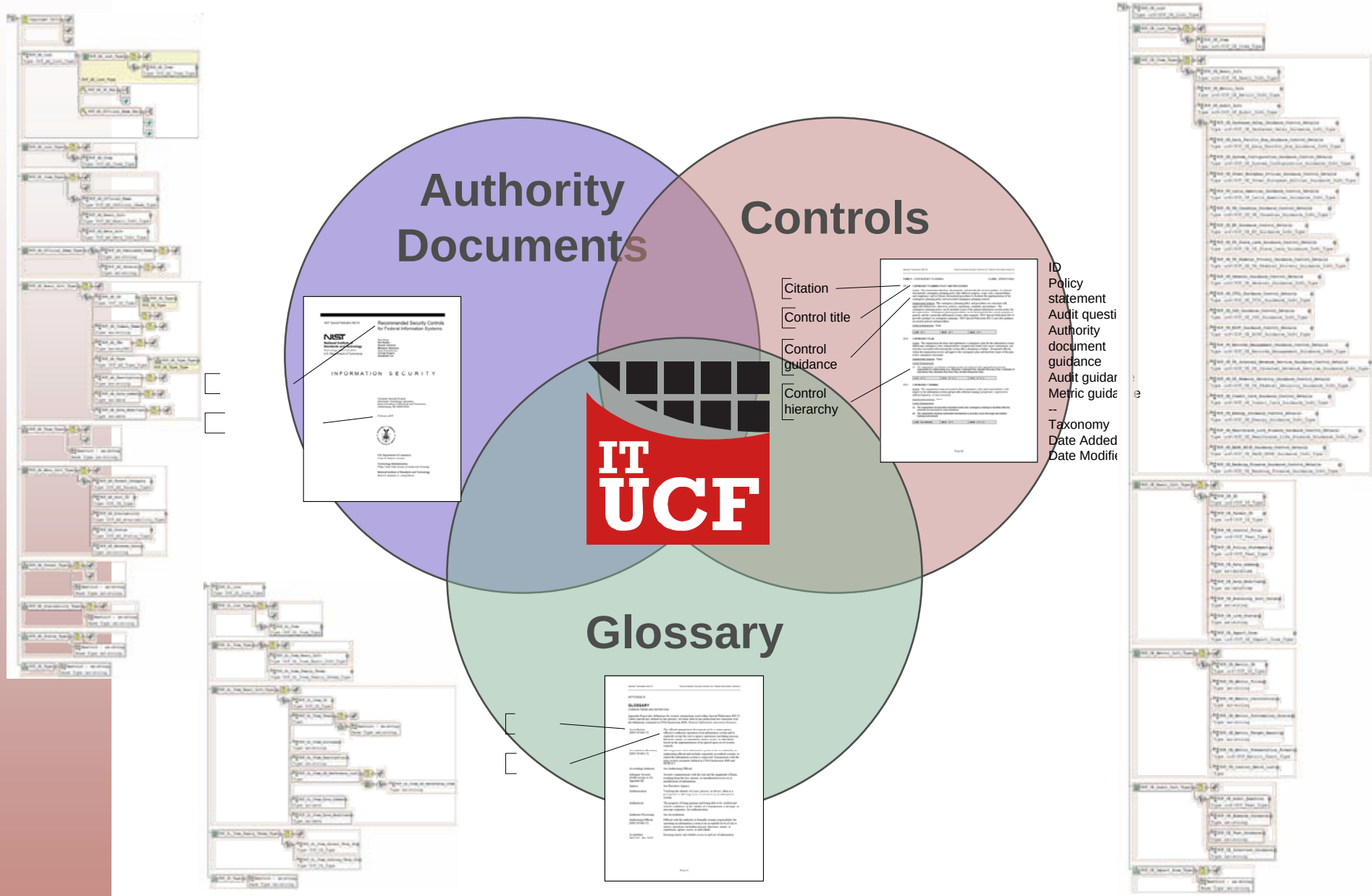
Maintain full documentation of all policies, standards, and procedures that support the compliance effort



And it has to accommodate *all* authority documents



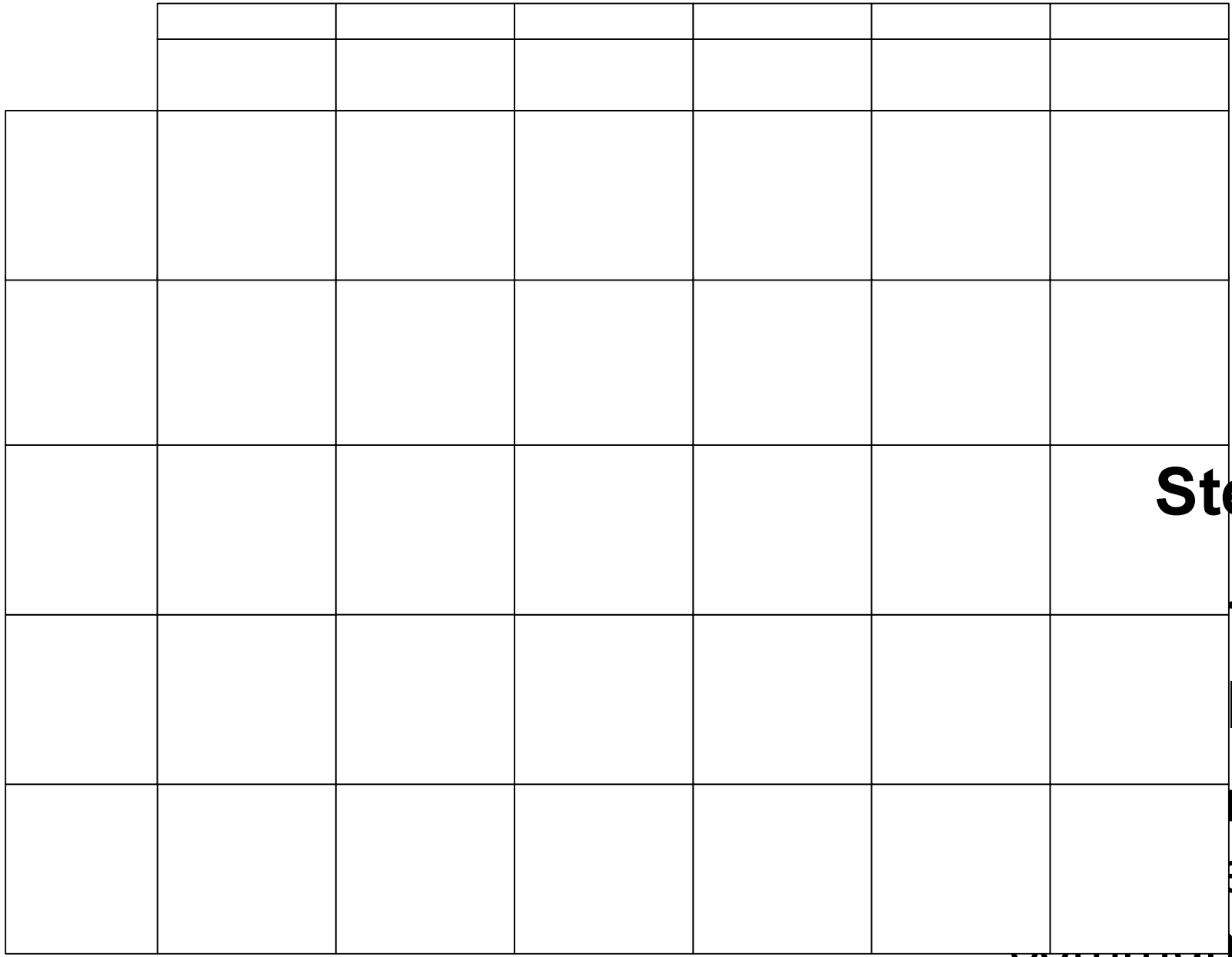
The UCF's public XML structures provide all three



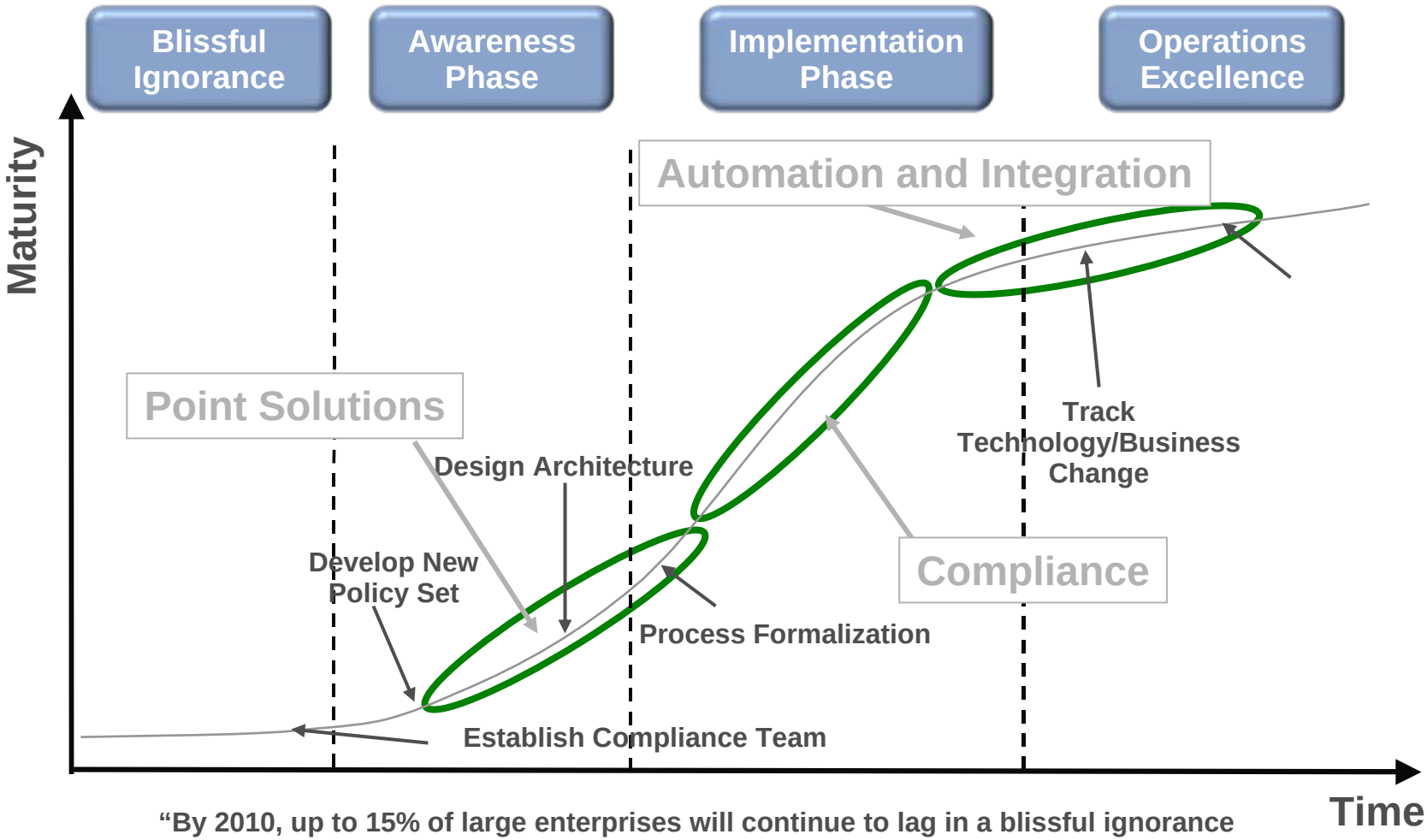
Beyond the Handshake Between Auditors and CMMI®

A Look Into Auditing for Process Maturity

Unified Compliance and CMMI



Where we want to get to (vs. where we are)



"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

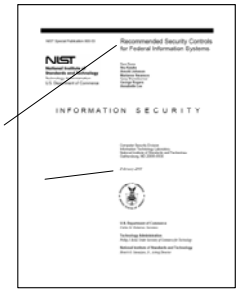
- There are 2407 **unique controls** identified to date

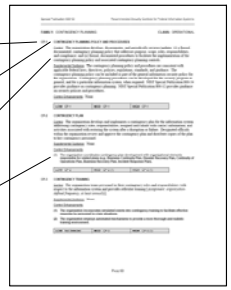
- There are 695 **matching audit questions** to date
- **Not one** of those audit questions asks about the *maturity* of the compliance process or provides a methodology for rating the maturity of the process

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

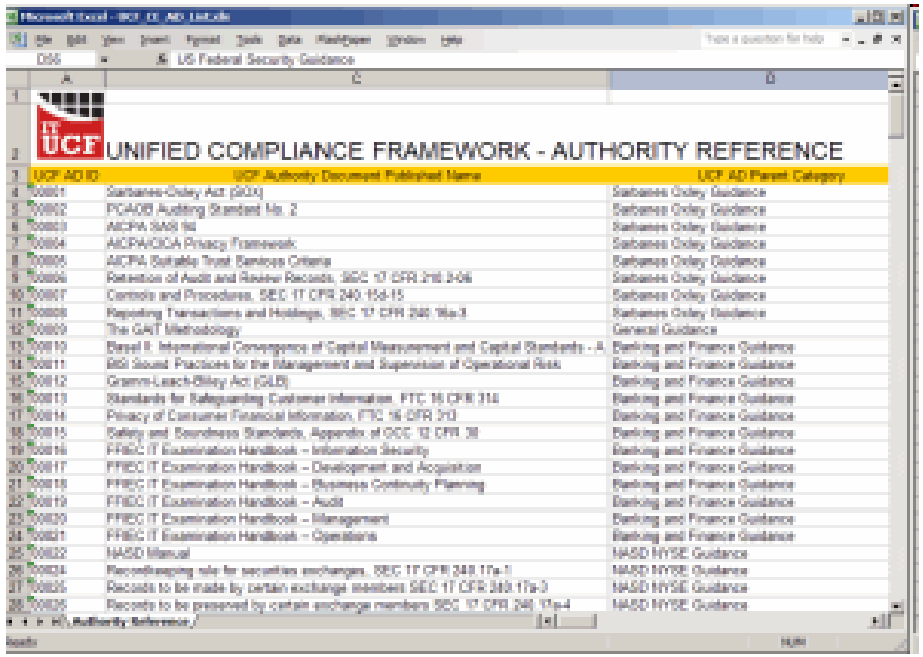
The Authority Document list

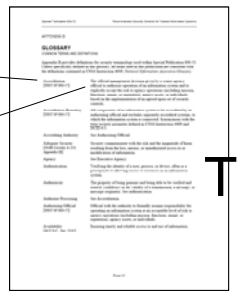




Citation
Control title
Control guidance
Control hierarchy

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



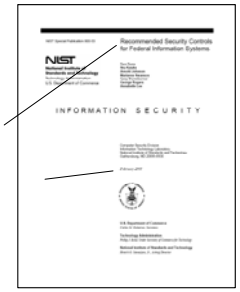


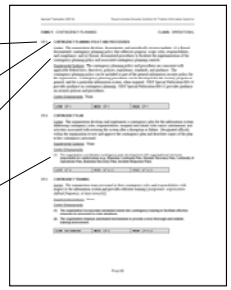
Title

ID
Common Name
URL
Type

Publicatio

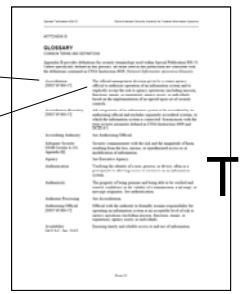
The Glossary





Citation
Control title
Control guidance
Control hierarchy

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



Title

Publicatio

HOME | ABOUT | PRESS | IMPACT ZONES | COMPLIANCE TOOLBOX | PARTNERS | BUY NOW

F

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. [Sedona Conference]

Fail safe

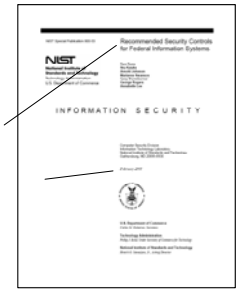
Automatic protection of programs and/or processing systems when hardware or software failure is detected. [US National Information Assurance (IA) Glossary]

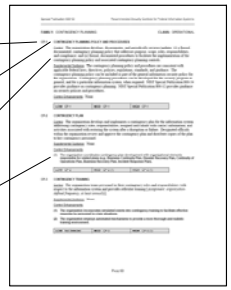
Fail soft

Selective termination of affected nonessential processing when hardware or software failure is determined to be imminent. [US National Information Assurance (IA) Glossary]

ID
Common Name
URL
Type

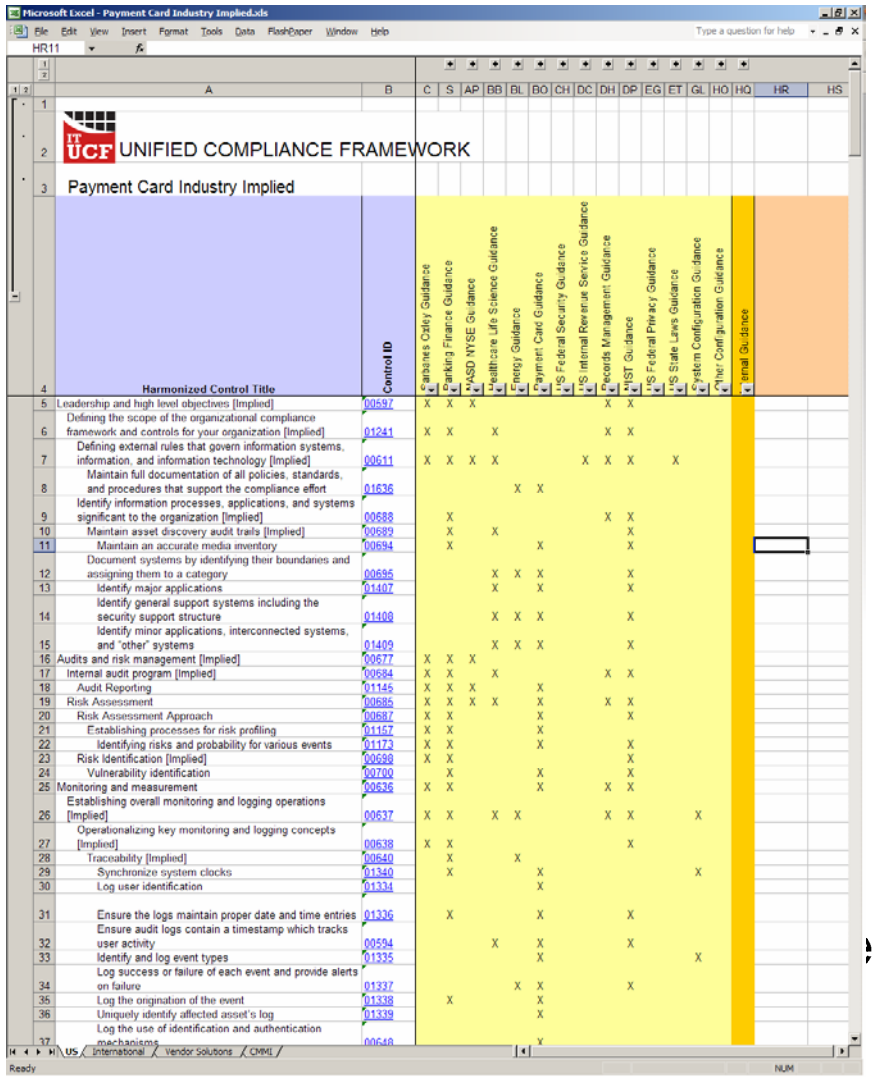
Harmonized control lists

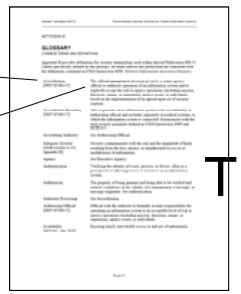




Citation
Control title
Control guidance
Control hierarchy

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





Title

Type

Publicatio

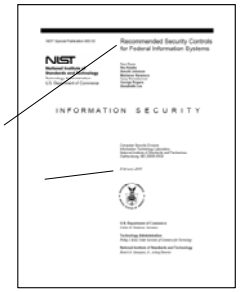
Responsibility and Accountability

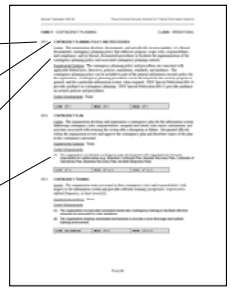
- ISACA and the IIA have huge quantities of documentation calling for a RACI assignment scheme

- **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

Step 1	**Step 2**	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	**Responsibility Accountability**	Policies and Procedures	Skills & Training	Tools & Automation	Measurement and Metrics

Harmonized work functions





Citation
Control title
Control guidance
Control hierarchy

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

Organizational work function description

Product/Solution Architecture Development

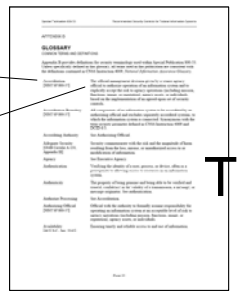
Control information		
Control ID:	Revision Date:	Revision Number:
Owner:		Approved By:

Controlled responsibilities

- Establish and maintain an information systems architecture metrics program [UCF Control ID 02059]

Non-controlled Responsibilities

- Lead the analyzing and designing solution structures process by capturing business and technical requirements from architectural and standards groups as well as interoperability requirements; drive the logical design process; provide a traceability map tracing features back to requirements and benefits; create the functional specifications; and define interim releases.
- Design/develop solutions concepts and align those concepts with the customer's enterprise architecture; devise versioned release strategy; and review plans for requirements capture.
- Define and manage project/solution scope and trade-off decisions through a triage process; manage project stakeholders expectations regarding solution content.
- Manage solution functional specifications and changes to the functional specifications; maintain traceability map; clarify the specification to other team roles and to external stakeholders; liaise with other project teams on interoperability issues.
- Provide update reports to enterprise architecture team; report on update requirements for future versioned releases.
- Provide uniform integration for legacy systems.



Common Name
URL
Type
Description
--
Title
Publication date

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	**Responsibility Accountability**	Policies and Procedures	Skills & Training	Tools & Automation	Measurement and Metrics

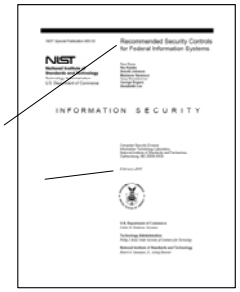
Policies and procedures

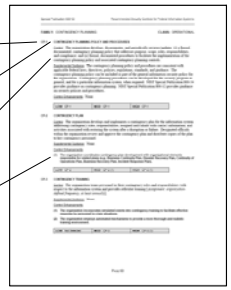
- This area is fully baked

- **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

Step 1	Step 2	**Step 3**	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	**Policies and Procedures**	Skills & Training	Tools & Automation	Measurement and Metrics

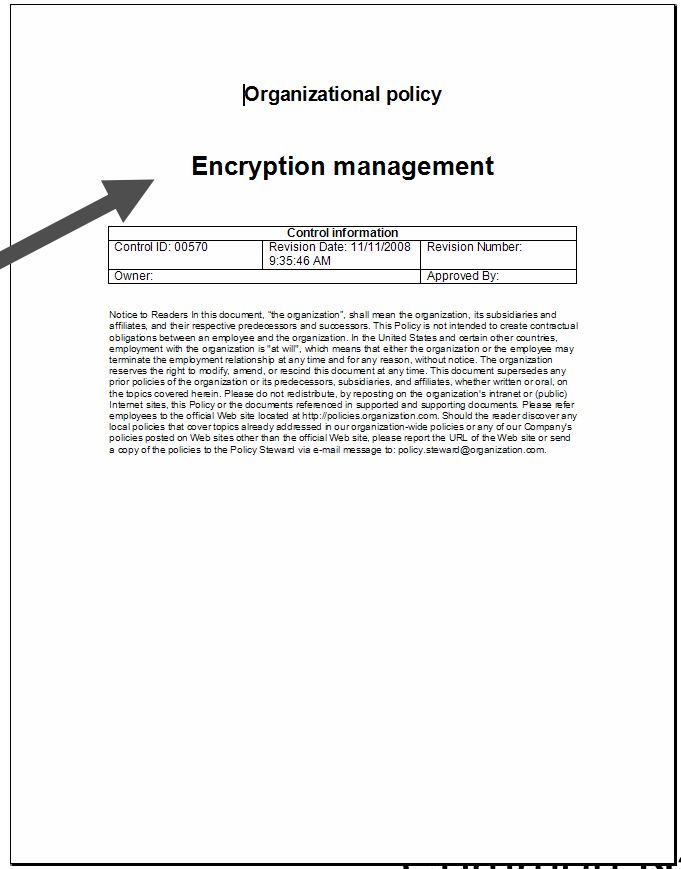
Ontologically-based policies





Citation
Control title
Control guidance
Control hierarchy

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

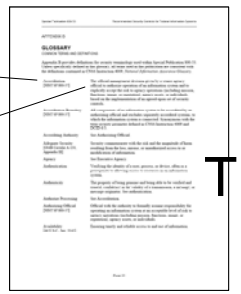


Organizational policy

Encryption management

Control information		
Control ID: 00570	Revision Date: 11/11/2008 9:35:46 AM	Revision Number:
Owner:		Approved By:

Notice to Readers In this document, "the organization", shall mean the organization, its subsidiaries and affiliates, and their respective predecessors and successors. This Policy is not intended to create contractual obligations between an employee and the organization. In the United States and certain other countries, employment with the organization is "at will", which means that either the organization or the employee may terminate the employment relationship at any time and for any reason, without notice. The organization reserves the right to modify, amend, or rescind this document at any time. This document supersedes any prior policies of the organization or its predecessors, subsidiaries, and affiliates, whether written or oral, on the topics covered herein. Please do not redistribute, by reposting on the organization's intranet or (public) Internet sites, this Policy or the documents referenced in supported and supporting documents. Please refer employees to the official Web site located at http://policies.organization.com. Should the reader discover any local policies that cover topics already addressed in our organization-wide policies or any of our Company's policies posted on Web sites other than the official Web site, please report the URL of the Web site or send a copy of the policies to the Policy Steward via e-mail message to: policy.steward@organization.com.



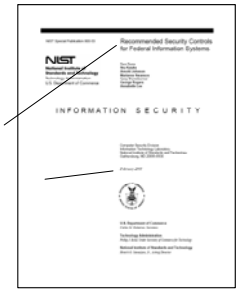
Title

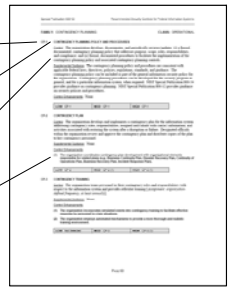
Publication date

Common Name
URL
Type
Description
--

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	**Policies and Procedures**	Skills & Training	Tools & Automation	Measurement and Metrics

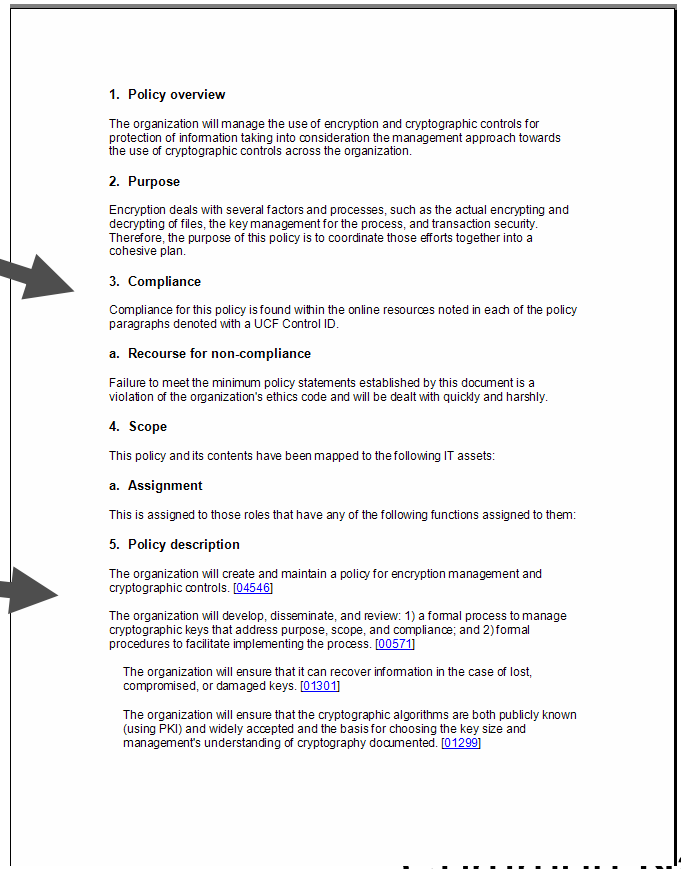
Ontologically-based policies





Citation
Control title
Control guidance
Control hierarchy

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



1. Policy overview

The organization will manage the use of encryption and cryptographic controls for protection of information taking into consideration the management approach towards the use of cryptographic controls across the organization.

2. Purpose

Encryption deals with several factors and processes, such as the actual encrypting and decrypting of files, the key management for the process, and transaction security. Therefore, the purpose of this policy is to coordinate those efforts together into a cohesive plan.

3. Compliance

Compliance for this policy is found within the online resources noted in each of the policy paragraphs denoted with a UCF Control ID.

a. Recourse for non-compliance

Failure to meet the minimum policy statements established by this document is a violation of the organization's ethics code and will be dealt with quickly and harshly.

4. Scope

This policy and its contents have been mapped to the following IT assets:

a. Assignment

This is assigned to those roles that have any of the following functions assigned to them:

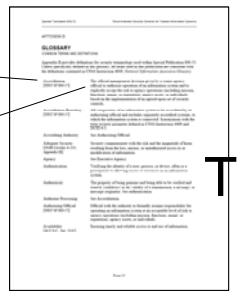
5. Policy description

The organization will create and maintain a policy for encryption management and cryptographic controls. [04546]

The organization will develop, disseminate, and review: 1) a formal process to manage cryptographic keys that address purpose, scope, and compliance; and 2) formal procedures to facilitate implementing the process. [00571]

The organization will ensure that it can recover information in the case of lost, compromised, or damaged keys. [01301]

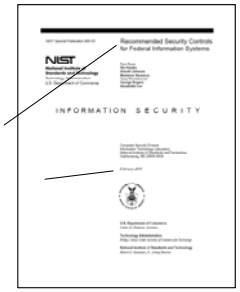
The organization will ensure that the cryptographic algorithms are both publicly known (using PKI) and widely accepted and the basis for choosing the key size and management's understanding of cryptography documented. [01299]

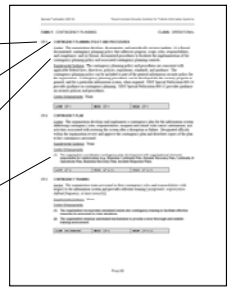


Title
Publication date
Common Name
URL
Type
Description
--

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	**Policies and Procedures**	Skills & Training	Tools & Automation	Measurement and Metrics

Ontologically-based policies





Citation
Control title
Control guidance
Control hierarchy

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

The organization will ensure that PKI authentication securely issues, updates, and unlock keys, provides for expiration of keys, ensures valid certificates, updates the list of revoked certificates, and logs the use of the root key. [01300]

The organization will restrict access to cryptographic keys to the fewest number of custodians necessary. [01297]

The organization will store cryptographic keys securely in the fewest possible locations and forms. [01298]

The organization will ensure that keys are changed periodically to ensure that they have not been compromised. [01302]

The organization will promptly destroy all cryptographic keys once their retention period had ended - ensuring that the destruction has been properly documented. [01303]

The organization will ensure that it requires 2 or 3 people, to control cryptographic keys, each knowing only their own part. [01304]

The organization will prevent the unauthorized substitution of cryptographic keys. [01305]

The organization will immediately replace, and document any suspected or compromised keys. [01306]

The organization will immediately revoke old or invalid keys. [01307]

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. [01308]

The organization will use strong cryptography and encryption techniques such as SSL, PPTP, and IPSEC to safeguard confidential data during transmission over public networks. [00564]

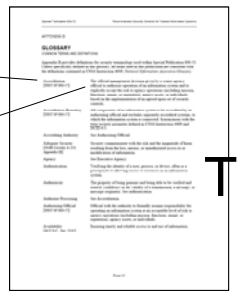
The organization will ensure that all confidential information is prohibited from being sent using either instant messaging or e-mail. [00565]

The organization will provide transaction authorization. [00566]

The organization will ensure non-repudiation. [00567]

The organization will ensure that all systems transmitting confidential information across public networks or wireless networks encrypt the transmissions using such techniques as VPNs, WPA for wireless, or SSL at 128-bit. [00568]

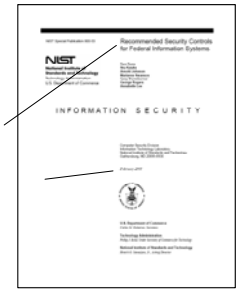
b. Supporting documents

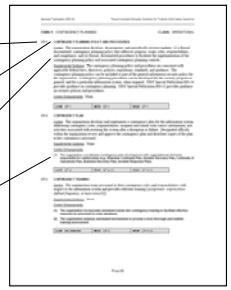


Title
Publication date
Common Name
URL
Type
Description
--

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	**Policies and Procedures**	Skills & Training	Tools & Automation	Measurement and Metrics

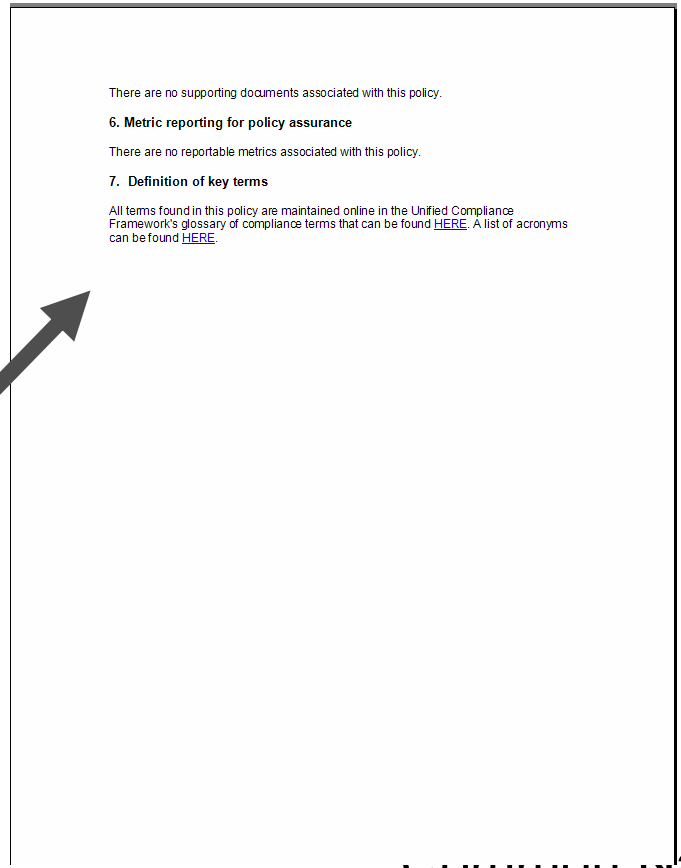
Ontologically-based policies





Citation
Control title
Control guidance
Control hierarchy

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



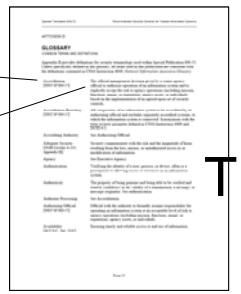
There are no supporting documents associated with this policy.

6. Metric reporting for policy assurance

There are no reportable metrics associated with this policy.

7. Definition of key terms

All terms found in this policy are maintained online in the Unified Compliance Framework's glossary of compliance terms that can be found HERE. A list of acronyms can be found HERE.



Title

Publication date

Common Name
URL
Type
Description
--

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	**Policies and Procedures**	Skills & Training	Tools & Automation	Measurement and Metrics

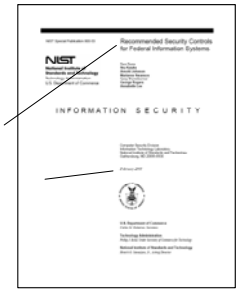
Skills and training

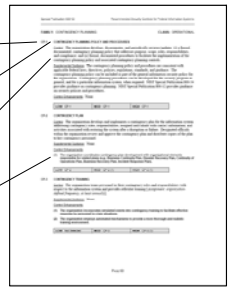
- Only those controls focused on training have a direct correlation

- **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

Step 1	Step 2	Step 3	**Step 4**	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	Policies and Procedures	**Skills & Training**	Tools & Automation	Measurement and Metrics

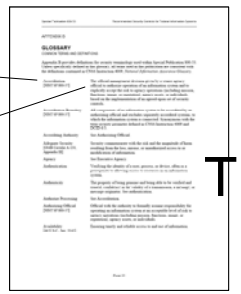
Not much is happening…





Citation
Control title
Control guidance
Control hierarchy

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



Title

Publication date

ID
Common Name
URL
Type
Description
--

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	Policies and Procedures	**Skills & Training**	Tools & Automation	Measurement and Metrics

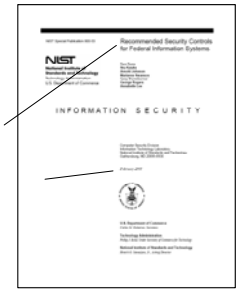
Tools and automation

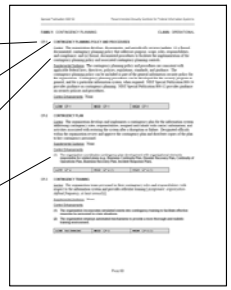
- Only those controls focused on tools have a direct correlation

- **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

Step 1	Step 2	Step 3	Step 4	**Step 5**	Step 6
Awareness and Acceptance	Responsibility Accountability	Policies and Procedures	Skills & Training	**Tools & Automation**	Measurement and Metrics

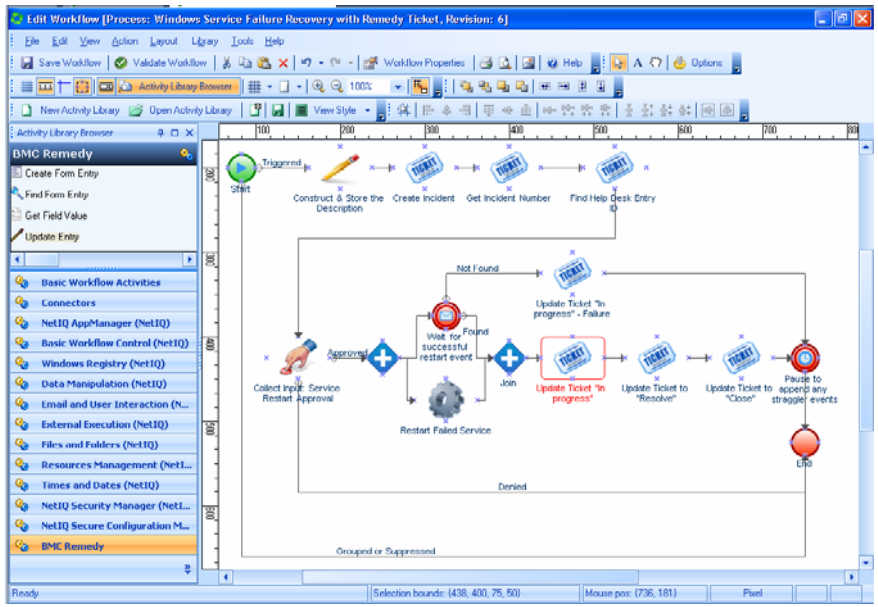
Process automation XML

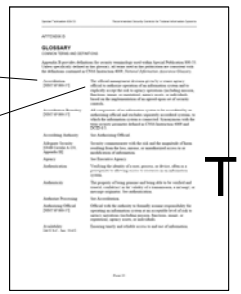




Citation
Control title
Control guidance
Control hierarchy

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





Title

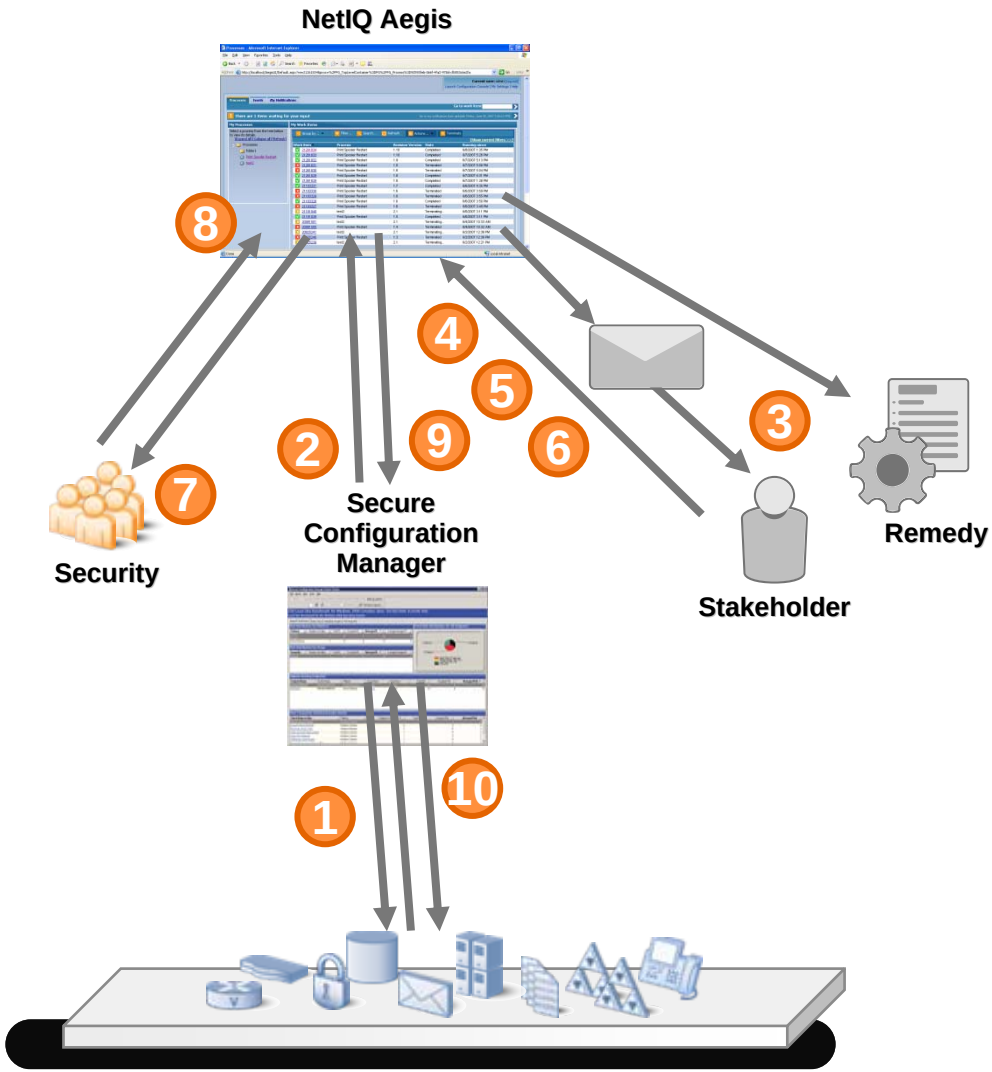
Publication date

ID
Common Name
URL
Type
Description

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	Policies and Procedures	Skills & Training	Tools & --Automation	Measurement and Metrics

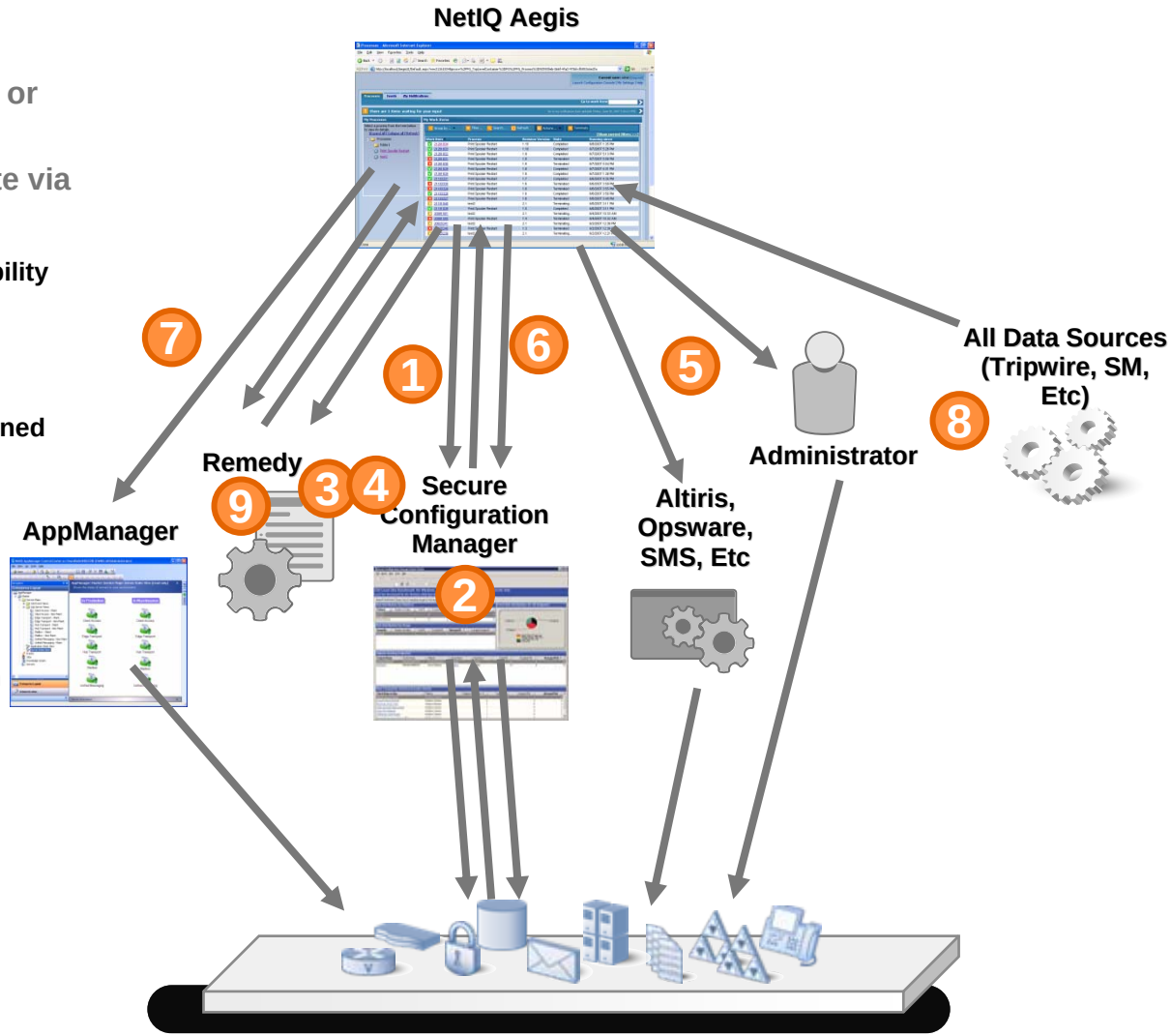
Closed loop exception management

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

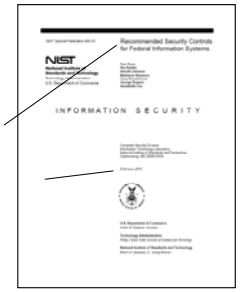


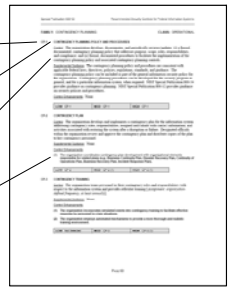
Closed loop vulnerability remediation

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



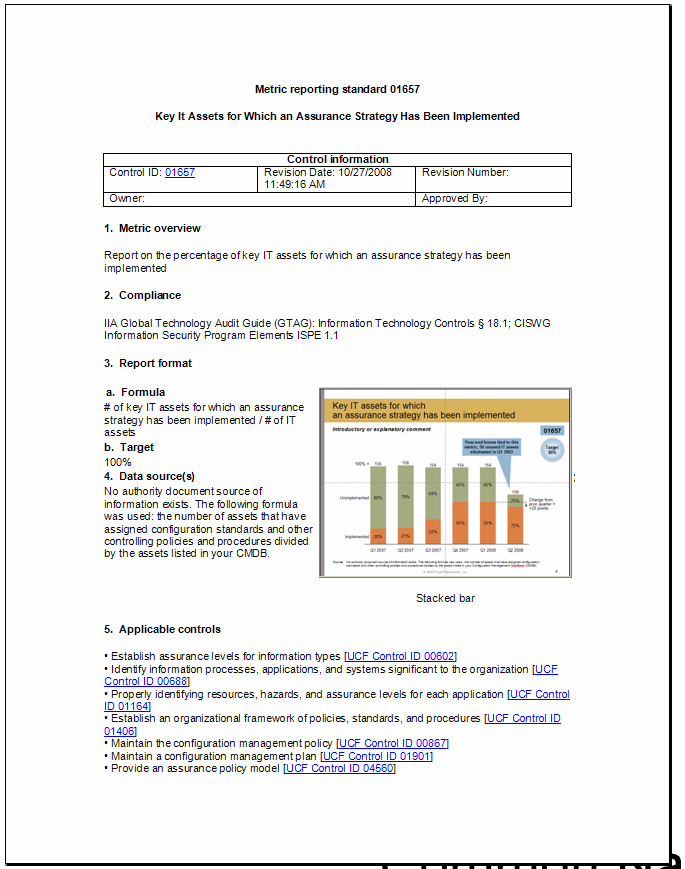
Defined metrics linked to defined controls





Citation
Control title
Control guidance
Control hierarchy

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



Metric reporting standard 01657

Key It Assets for Which an Assurance Strategy Has Been Implemented

Control information		
Control ID: 01657	Revision Date: 10/27/2008 11:49:16 AM	Revision Number:
Owner:		Approved By:

1. Metric overview

Report on the percentage of key IT assets for which an assurance strategy has been implemented

2. Compliance

IIA Global Technology Audit Guide (GTAG): Information Technology Controls § 18.1; CISWG Information Security Program Elements ISPE 1.1

3. Report format

a. Formula
# of key IT assets for which an assurance strategy has been implemented / # of IT assets

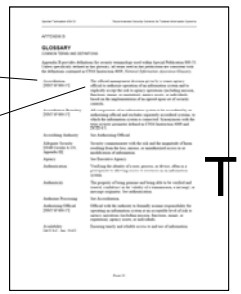
b. Target
100%

4. Data source(s)
No authority document source of information exists. The following formula was used: the number of assets that have assigned configuration standards and other controlling policies and procedures divided by the assets listed in your CMDB.

Stacked bar

5. Applicable controls

- Establish assurance levels for information types [UCF Control ID 00602]
- Identify information processes, applications, and systems significant to the organization [UCF Control ID 00688]
- Properly identifying resources, hazards, and assurance levels for each application [UCF Control ID 01164]
- Establish an organizational framework of policies, standards, and procedures [UCF Control ID 01406]
- Maintain the configuration management policy [UCF Control ID 00867]
- Maintain a configuration management plan [UCF Control ID 01901]
- Provide an assurance policy model [UCF Control ID 04560]



Title
Publication date
Common Name
URL
Type
Description
--

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Awareness and Acceptance	Responsibility Accountability	Policies and Procedures	Skills & Training	Tools & Automation	Measurement and Metrics

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

Step 1	Step 2	Step 3	Step 4	Step 5	**Step 6**
Awareness and Acceptance	Responsibility Accountability	Policies and Procedures	Skills & Training	Tools & Automation	**Measurement and Metrics**