Micro Craft, Inc.

NDIA Procurement Division
Cyber DFARS Workshop

Mr. Steve Gleason, CISSP
January 9, 2018

Micro Craft History

Proud to be 100% Employee Owned

- Founded in 1958 by craftsman Charles Folk

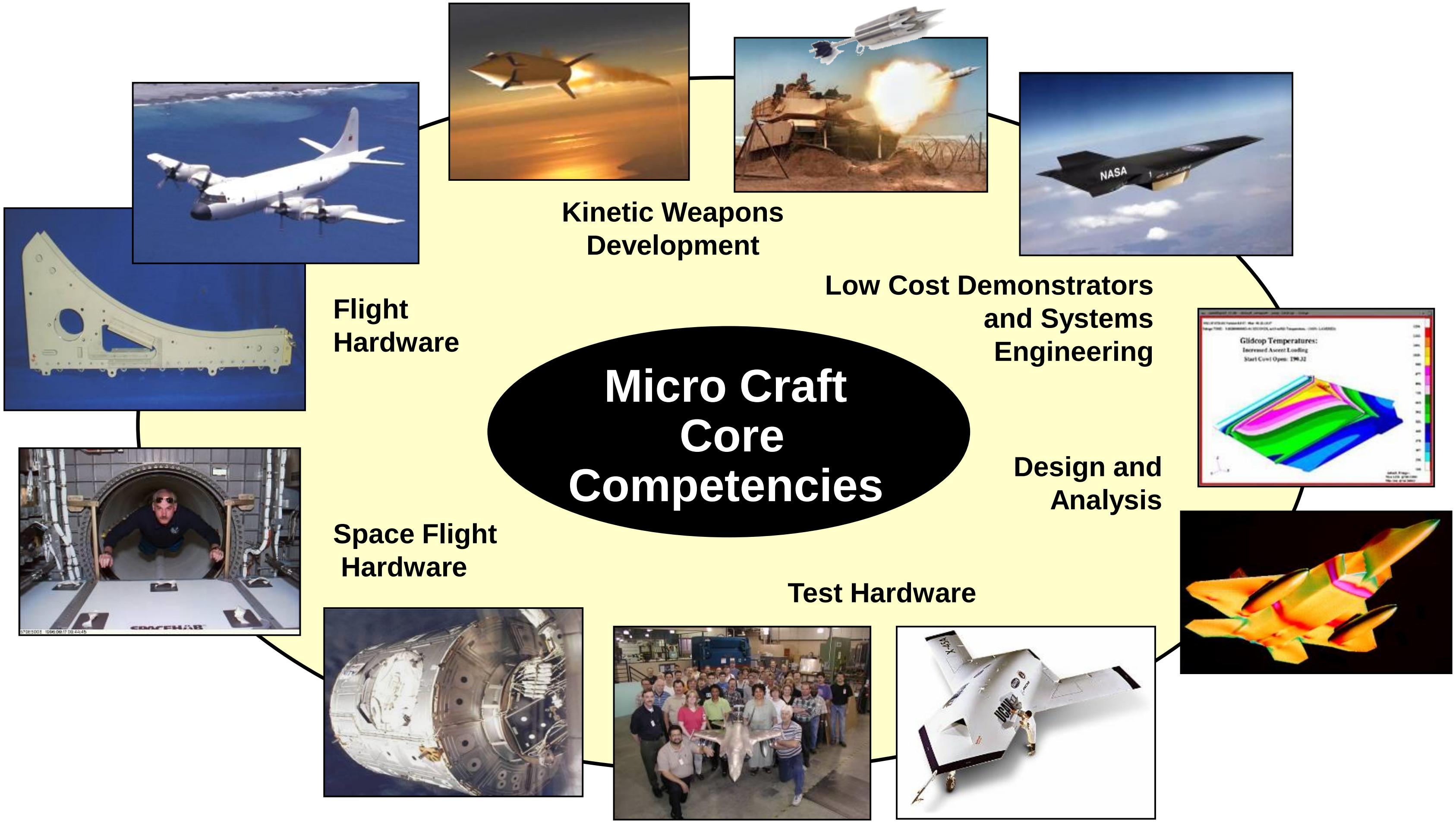
- Key provider of complex wind tunnel models and other specialty hardware – pioneers in CNC, EDM, etc.

- Rapid expansion in 1990s into space and technology markets

- Prime contractor and vehicle manufacturer and integrator for NASA’s X-43A and X-43C Hyper-X Programs

- After a brief period of ownership by an investment group, Micro Craft was acquired by ATK in 2003.
- In 2011, Micro Craft was acquired by its employees and became a **100% Employee-owned Small Business**.

Micro Craft Core Competencies



Micro Craft Core Competencies

Kinetic Weapons Development

Flight Hardware

Low Cost Demonstrators and Systems Engineering

Design and Analysis

Space Flight Hardware

Test Hardware

Development, Engineer, Test, and Manufacture

Business Overview and Environment

Company

- 60+ employees, 40 of which are owners
- Manufacturing Craftsmen and CNC operators, Manufacturing Management, Engineers, Estimators, Accounting, Contracts, Security, IT, Business Development, Executive Management

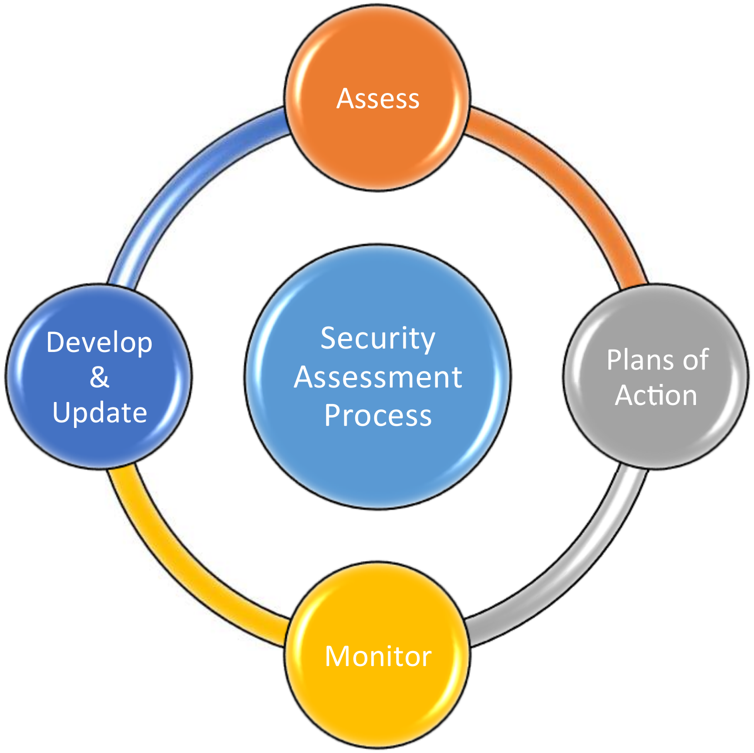
Business Base

- DoD classified and unclassified programs
- Commercial projects

Information System / Data

- On-premise servers and workstations
- Virtual server farm
- Variety of workstation classes
- Engineering and design technical data

Assessment Process



Assess

Plans of Action

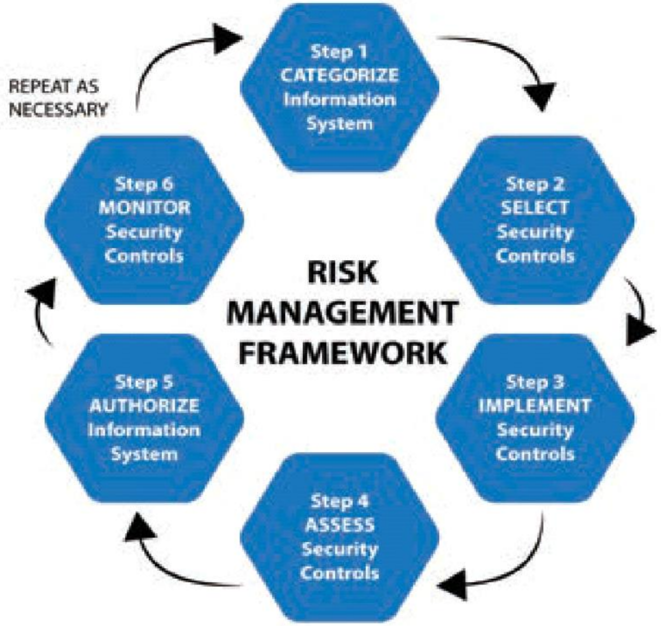
Monitor

Develop & Update

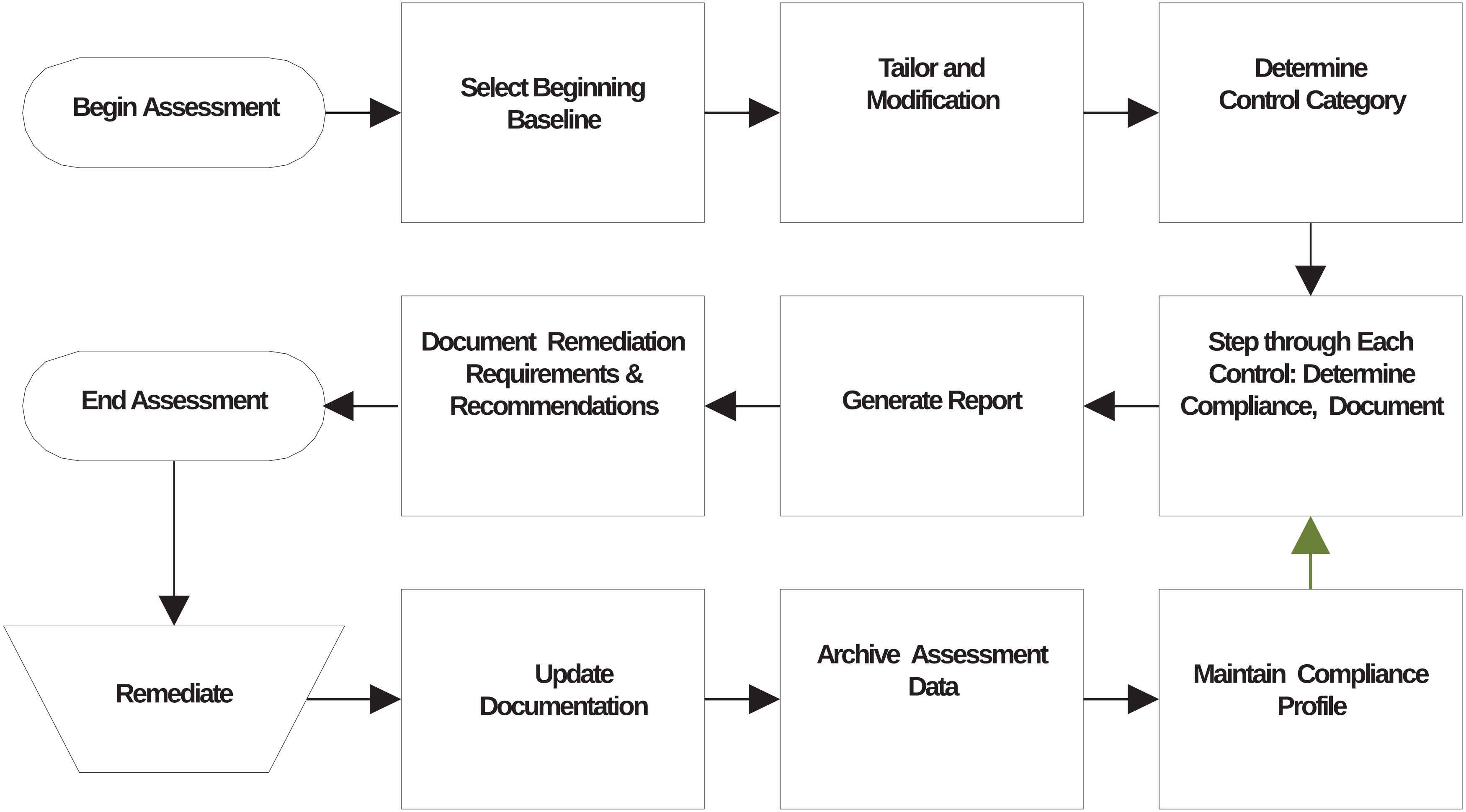
Security Assessment Process

Compliance Team

- CEO
- HR
- FSO
- Contracts
- CIO


REPEAT AS NECESSARY
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

Continuous Assessment Flow



Begin Assessment

Select Beginning Baseline

Tailor and Modification

Determine Control Category

Step through Each Control: Determine Compliance, Document

Generate Report

Document Remediation Requirements & Recommendations

End Assessment

Remediate

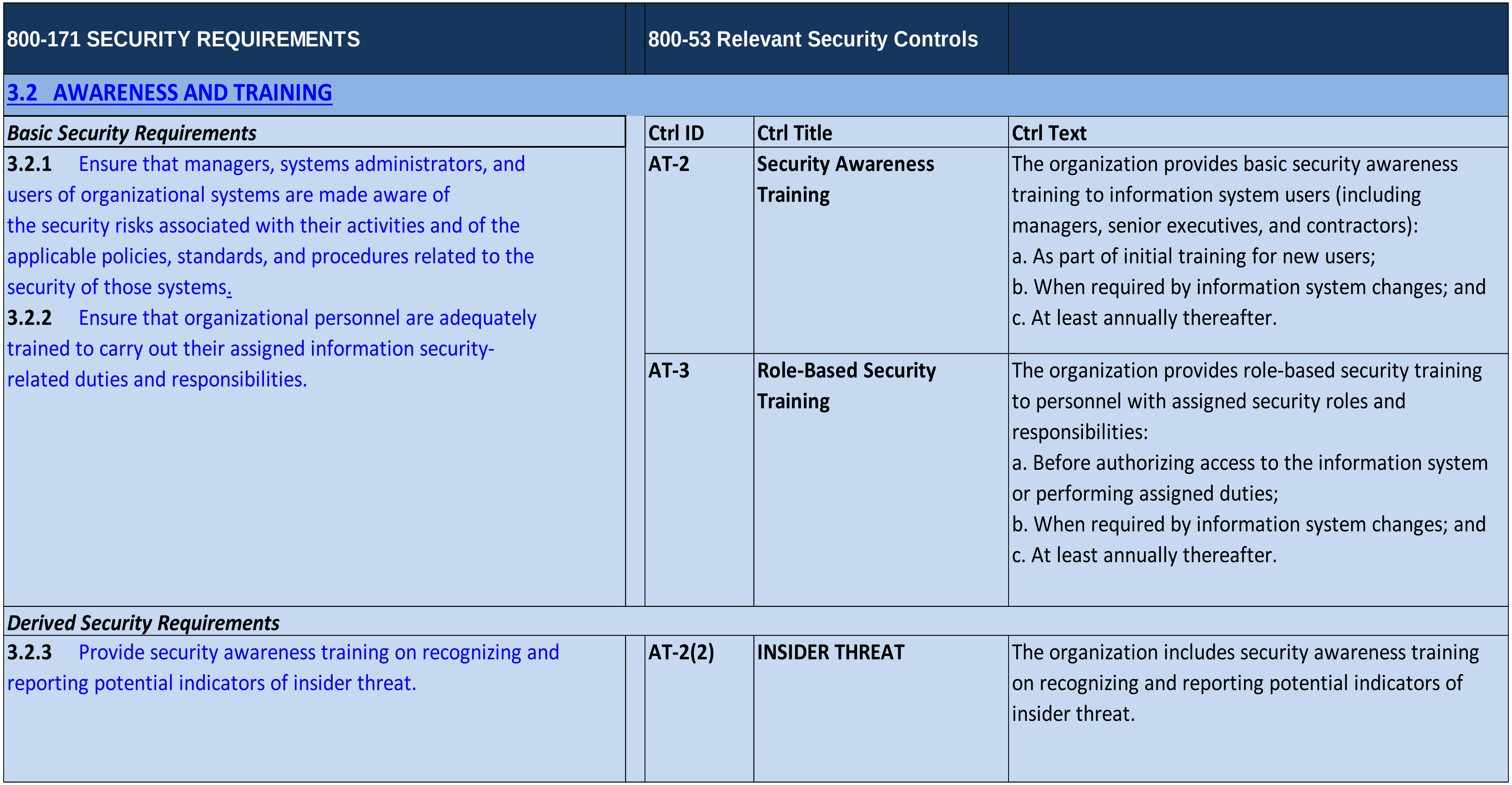
Update Documentation

Archive Assessment Data

Maintain Compliance Profile

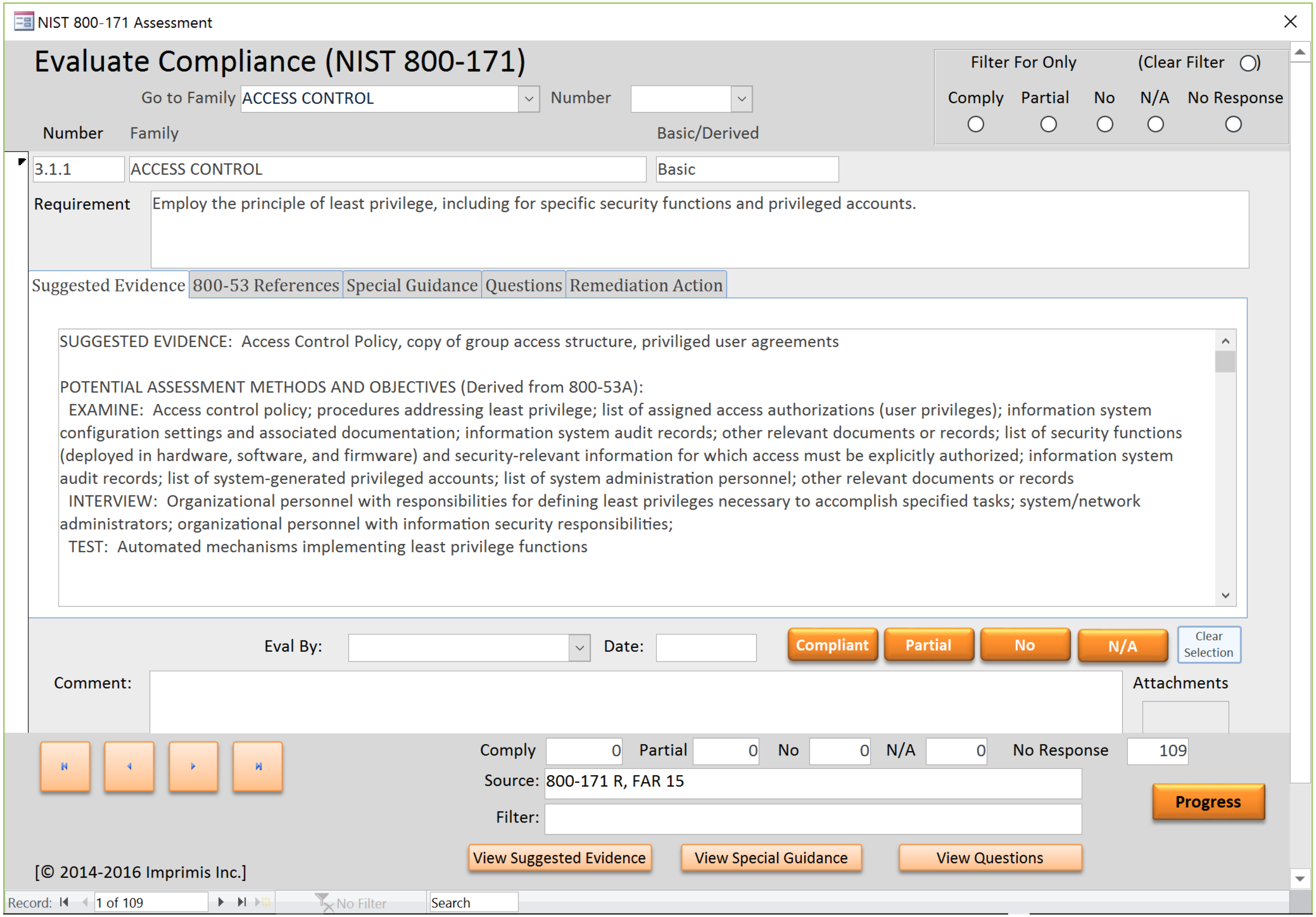
Control Inventory

- **Crosswalk 800-171 to 800-53**



800-171 SECURITY REQUIREMENTS	800-53 Relevant Security Controls		
3.2 AWARENESS AND TRAINING			
Basic Security Requirements	**Ctrl ID**	**Ctrl Title**	**Ctrl Text**
3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. **3.2.2** Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	**AT-2**	**Security Awareness Training**	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. At least annually thereafter.
	AT-3	**Role-Based Security Training**	The organization provides role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. At least annually thereafter.
Derived Security Requirements			
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	**AT-2(2)**	**INSIDER THREAT**	The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

Self Assessment - Evidence



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family ACCESS CONTROL   Number

Filter For Only   (Clear Filter ○)

Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

SUGGESTED EVIDENCE: Access Control Policy, copy of group access structure, priviliged user agreements

POTENTIAL ASSESSMENT METHODS AND OBJECTIVES (Derived from 800-53A):

EXAMINE: Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; information system audit records; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records

INTERVIEW: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; system/network administrators; organizational personnel with information security responsibilities;

TEST: Automated mechanisms implementing least privilege functions

Eval By: Date:

Comment:

Attachments

Comply 0   Partial 0   No 0   N/A 0   No Response 109

Source: 800-171 R, FAR 15

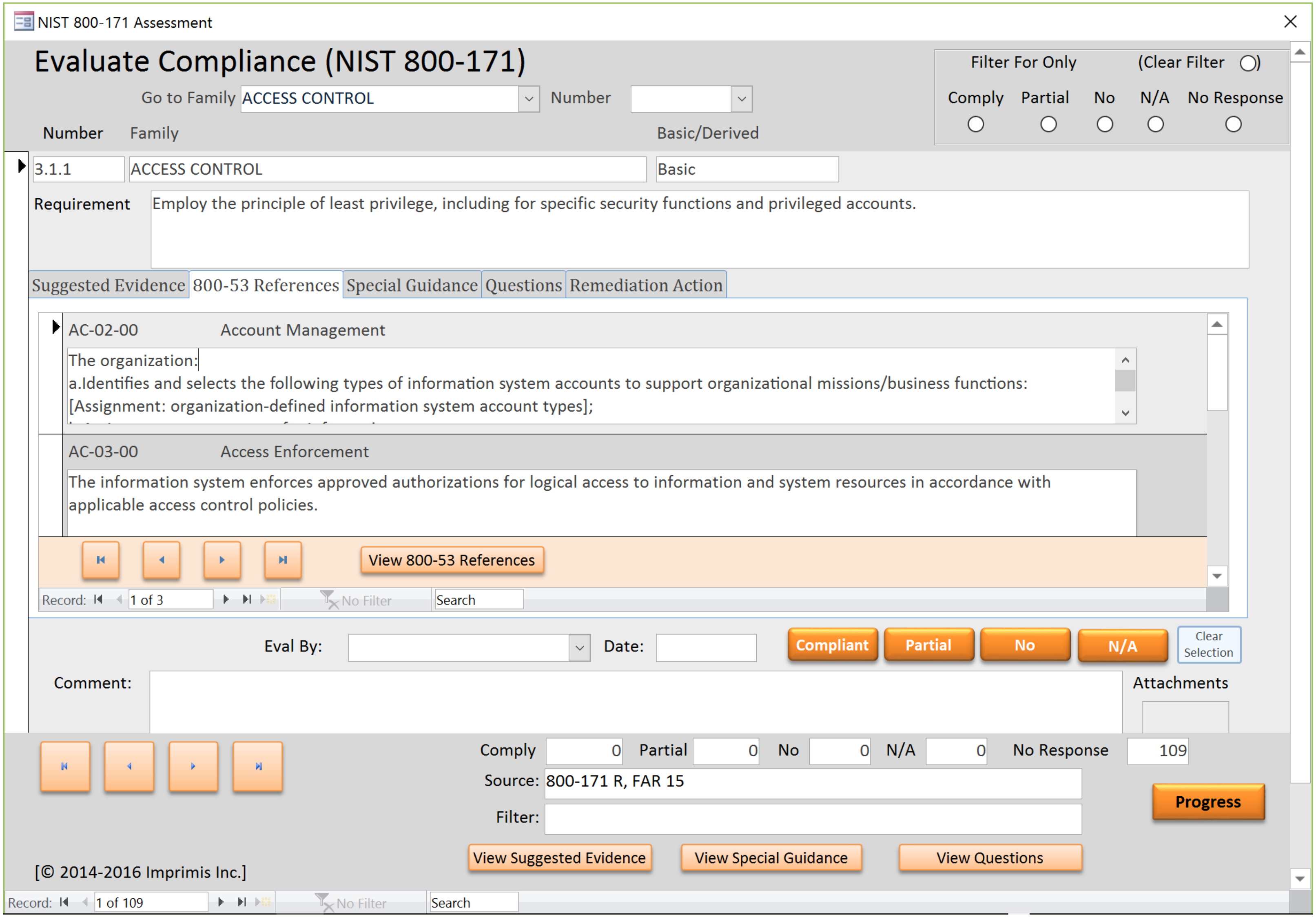
Filter:

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109   No Filter   Search

Self Assessment – 800-53 Reference

Proud to be 100% Employee Owned



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL

Number:

Filter For Only (Clear Filter ○)

Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

Suggested Evidence | 800-53 References | Special Guidance | Questions | Remediation Action

AC-02-00 Account Management

The organization:
a.Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

AC-03-00 Access Enforcement

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Record: 1 of 3 No Filter Search

Eval By:

Date:

Comment:

Attachments

Comply	Partial	No	N/A	No Response
0	0	0	0	109

Source: 800-171 R, FAR 15

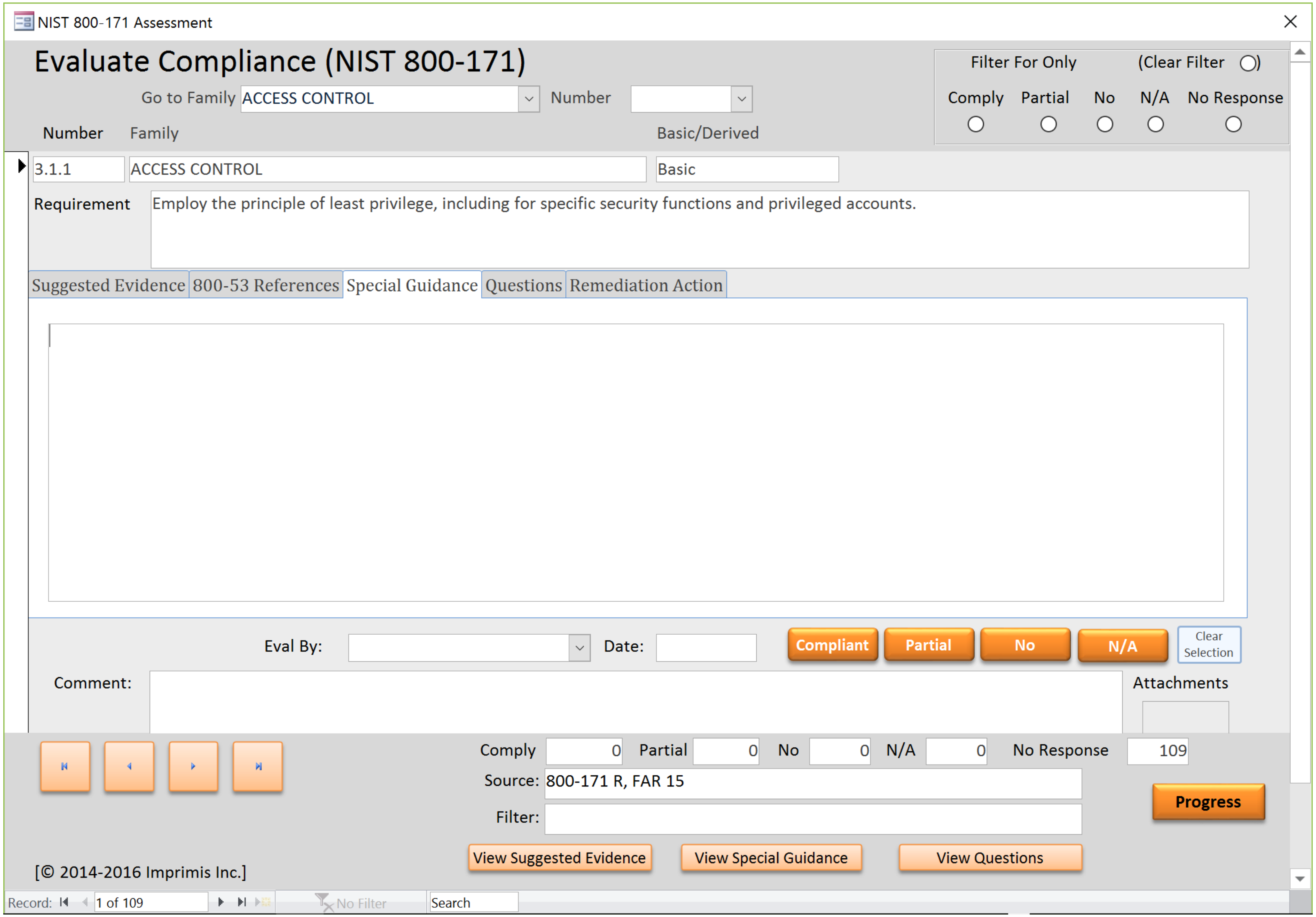
Filter:

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109 No Filter Search

Self Assessment - Guidance

Proud to be 100% Employee Owned



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: ACCESS CONTROL
Number:

Filter For Only (Clear Filter ○)
Comply ○ Partial ○ No ○ N/A ○ No Response ○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

Requirement: Employ the principle of least privilege, including for specific security functions and privileged accounts.

Eval By:
Date:

Comment:
Attachments

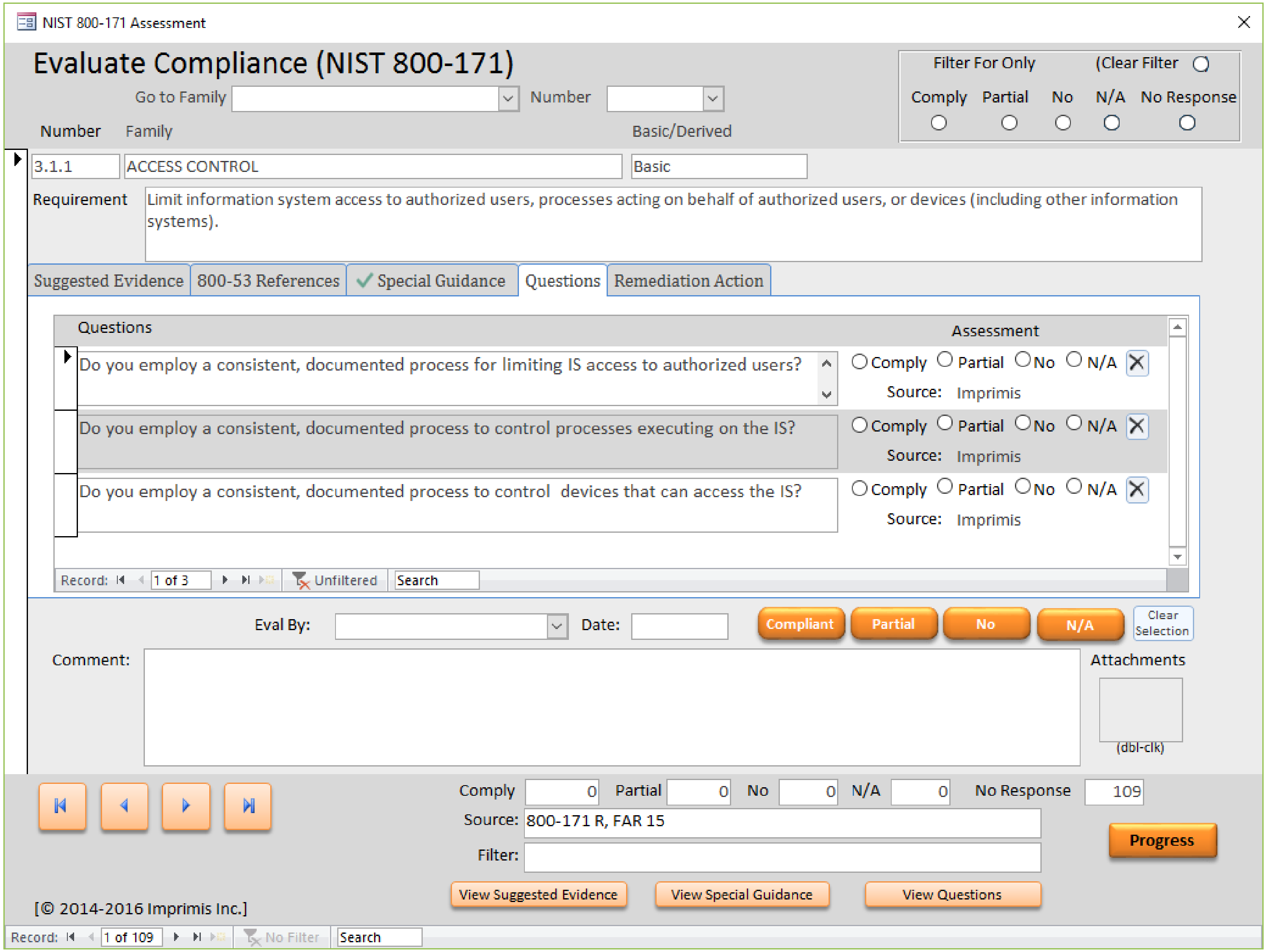
Comply	0	Partial	0	No	0	N/A	0	No Response	109

Source: 800-171 R, FAR 15
Filter:

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109

Self Assessment - Questions



NIST 800-171 Assessment

Evaluate Compliance (NIST 800-171)

Go to Family: | Number:

Filter For Only				(Clear Filter ○
Comply	Partial	No	N/A	No Response
○	○	○	○	○

Number	Family	Basic/Derived
3.1.1	ACCESS CONTROL	Basic

Requirement: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

Suggested Evidence | 800-53 References | ✓ Special Guidance | Questions | Remediation Action

Questions	Assessment
Do you employ a consistent, documented process for limiting IS access to authorized users?	○ Comply ○ Partial ○ No ○ N/A ☒ Source: Imprimis
Do you employ a consistent, documented process to control processes executing on the IS?	○ Comply ○ Partial ○ No ○ N/A ☒ Source: Imprimis
Do you employ a consistent, documented process to control devices that can access the IS?	○ Comply ○ Partial ○ No ○ N/A ☒ Source: Imprimis

Record: 1 of 3 | Unfiltered | Search

Eval By: | Date:

Compliant | Partial | No | N/A | Clear Selection

Comment:

Attachments (dbl-clk)

Comply	Partial	No	N/A	No Response
0	0	0	0	109

Source: 800-171 R, FAR 15

Filter:

Progress

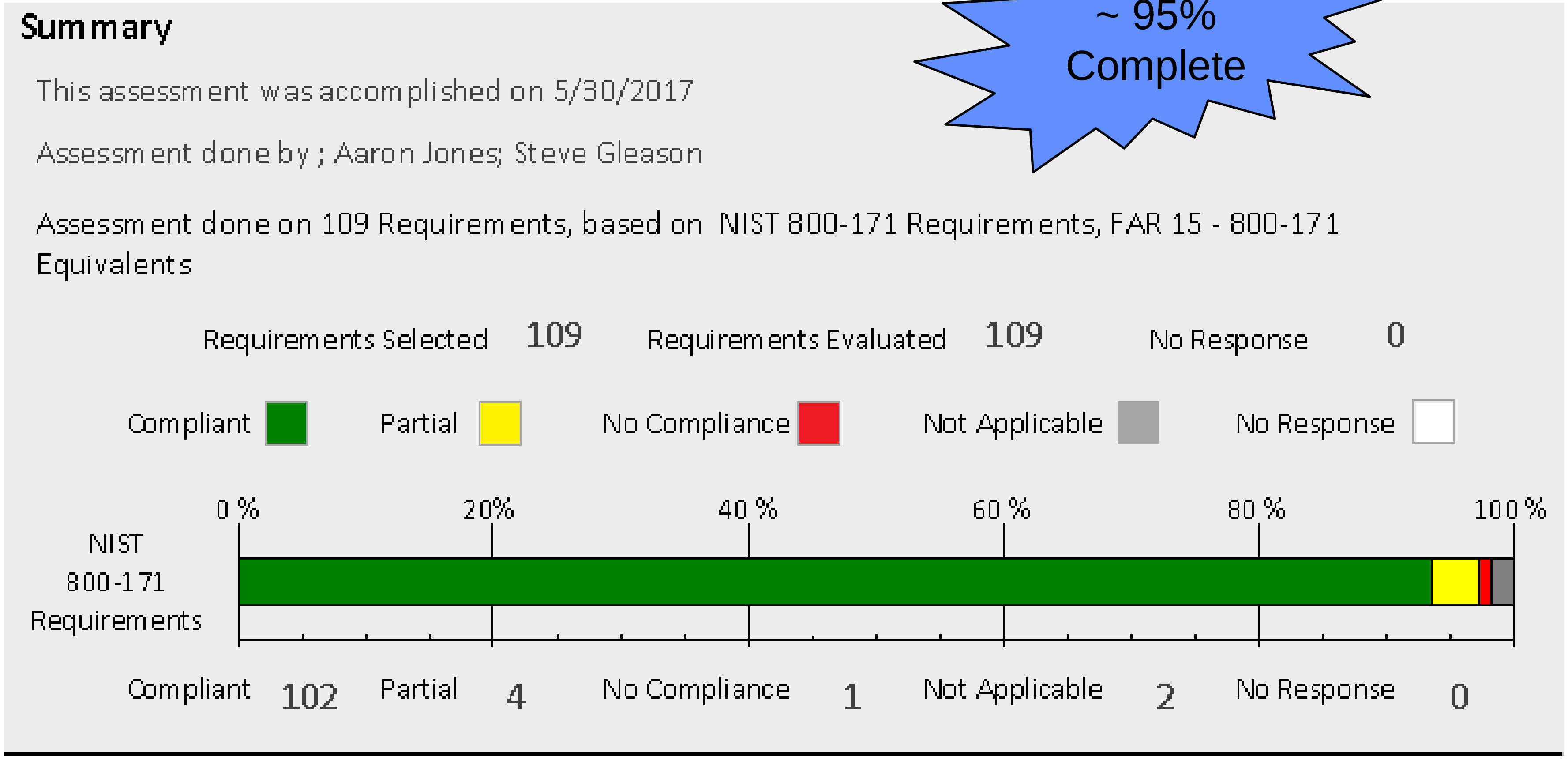
View Suggested Evidence | View Special Guidance | View Questions

[© 2014-2016 Imprimis Inc.]

Record: 1 of 109 | No Filter | Search

Self Assessment – Compliance Summary

~ 95%
Complete



Summary

This assessment was accomplished on 5/30/2017

Assessment done by ; Aaron Jones; Steve Gleason

Assessment done on 109 Requirements, based on NIST 800-171 Requirements, FAR 15 - 800-171 Equivalents

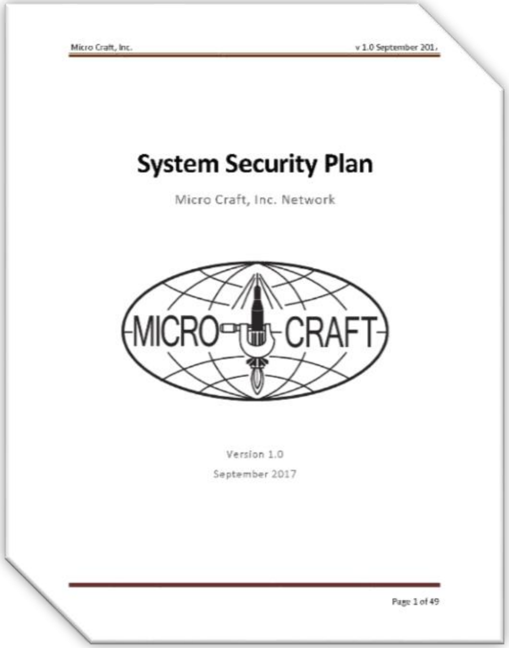
Requirements Selected	109	Requirements Evaluated	109	No Response	0

Compliant 🟩 Partial 🟨 No Compliance 🟥 Not Applicable ▨ No Response □

Compliant	102	Partial	4	No Compliance	1	Not Applicable	2	No Response	0

Compliance Documentation

- **SSP – System Security Plan**
- **POA&M – Plan of Actions and Milestones**



Micro Craft, Inc. v 1.0 September 201

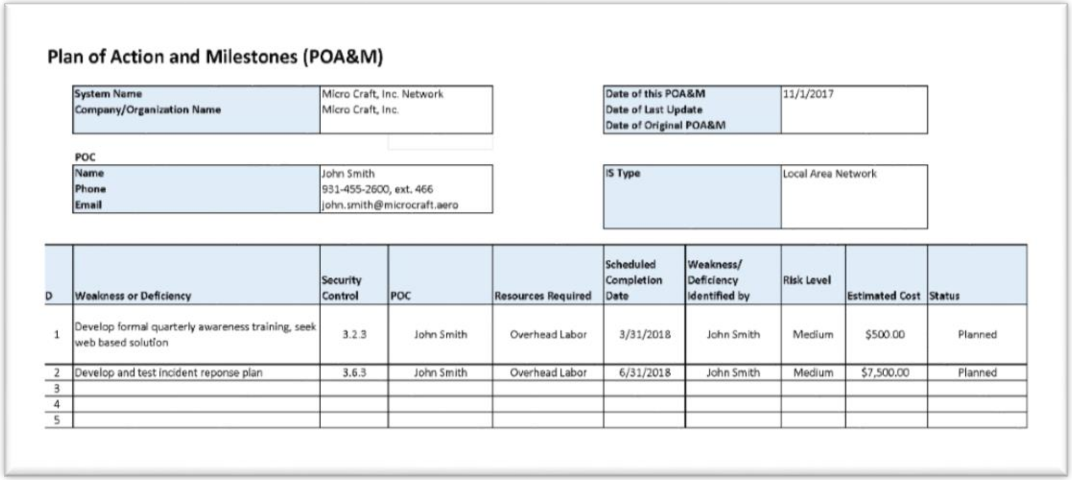
System Security Plan

Micro Craft, Inc. Network

Version 1.0

September 2017

Page 1 of 49



Plan of Action and Milestones (POA&M)

System Name	Micro Craft, Inc. Network
Company/Organization Name	Micro Craft, Inc.

Date of this POA&M	11/1/2017
Date of Last Update	
Date of Original POA&M	

POC

Name	John Smith
Phone	931-455-2600, ext. 466
Email	john.smith@microcraft.aero

IS Type	Local Area Network

D	Weakness or Deficiency	Security Control	POC	Resources Required	Scheduled Completion Date	Weakness/ Deficiency Identified by	Risk Level	Estimated Cost	Status
1	Develop formal quarterly awareness training, seek web based solution	3.2.3	John Smith	Overhead Labor	3/31/2018	John Smith	Medium	$500.00	Planned
2	Develop and test incident reponse plan	3.6.3	John Smith	Overhead Labor	6/31/2018	John Smith	Medium	$7,500.00	Planned
3									
4									
5									

System Security Plan

A document that describes how a small manufacturer meets the security requirements for a system or how a small manufacturer plans to meet the requirements.

The system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.

Micro Craft, Inc. v 1.0 September 2017

System Security Plan

Micro Craft, Inc. Network

Version 1.0

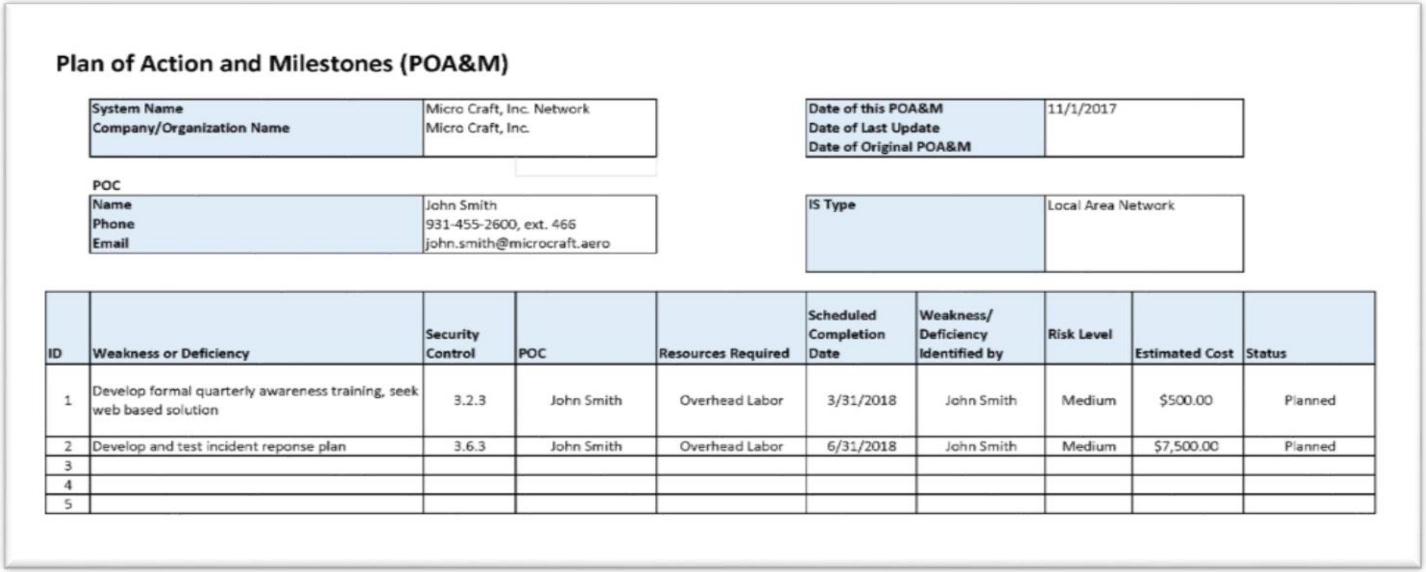
September 2017

Page 1 of 49

What are Plans of Action?

Describes how many unimplemented security requirements will be met and how any planned mitigations will be implemented. Companies can document the system security plan and plan of action as separate or combined documents and in any chosen format.

When requested, the System Security plan and any associated Plans of Action for any planned implementations or mitigations should be submitted.



Plan of Action and Milestones (POA&M)

System Name	Micro Craft, Inc. Network
Company/Organization Name	Micro Craft, Inc.

Date of this POA&M	11/1/2017
Date of Last Update	
Date of Original POA&M	

POC

Name	John Smith
Phone	931-455-2600, ext. 466
Email	john.smith@microcraft.aero

IS Type	Local Area Network

ID	Weakness or Deficiency	Security Control	POC	Resources Required	Scheduled Completion Date	Weakness/ Deficiency Identified by	Risk Level	Estimated Cost	Status
1	Develop formal quarterly awareness training, seek web based solution	3.2.3	John Smith	Overhead Labor	3/31/2018	John Smith	Medium	$500.00	Planned
2	Develop and test incident reponse plan	3.6.3	John Smith	Overhead Labor	6/31/2018	John Smith	Medium	$7,500.00	Planned
3									
4									
5									

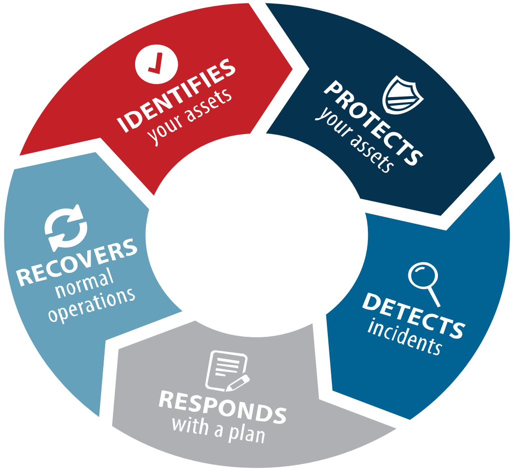
Implementation of SSP

Resulting Documentation

- Departmental Interviews
- Gather Existing Policies and Procedures
- Create Policies and Procedures
- Awareness and Training

Technologies to meet controls

- Vulnerability Scanning
- Patch Management
- Endpoint Management
- Firewall Configuration
- Group Policies



Assessment / Implementation Notes

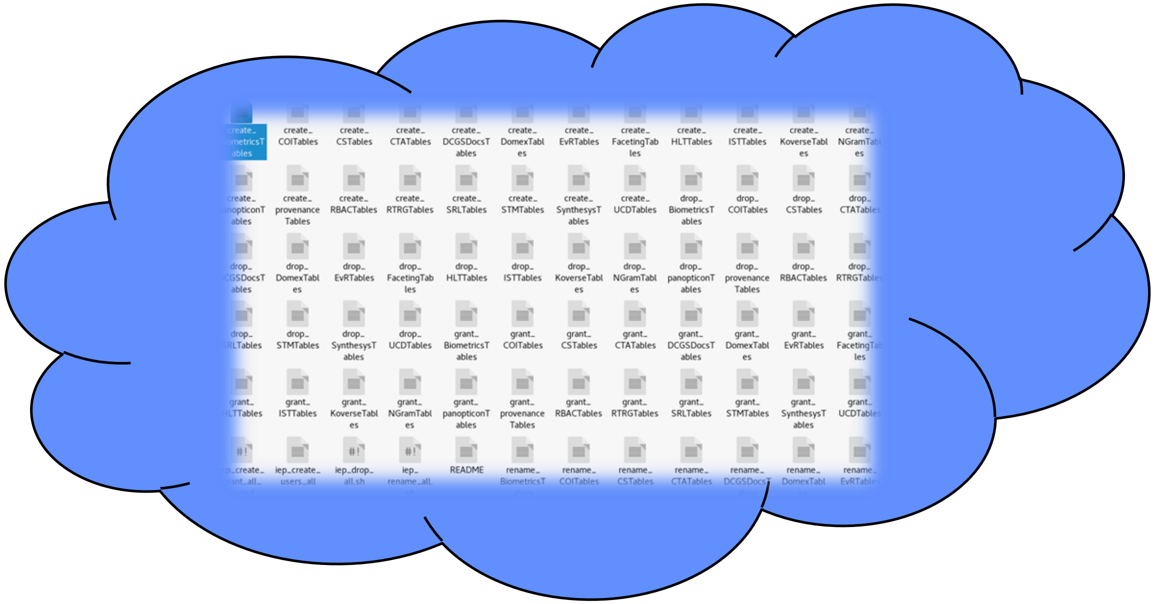
- **Identify low hanging fruit along the way**
  - Administrative (upgrade / ”tweak” existing systems)
  - Review / “Lean-out” business processes
- **Prepare and respond to control’s impact on users**
  - Supporting users in a small business is a unique challenge
  - Attitudes toward new security controls will not change over night
  - Regular group communication either through email or formal training sessions are critical to timely implementation of security controls.
  - Most small business users wear multiple hats
  - Controls will expose processes that must be altered and improved (document)

Supporting Implementation Activities

- Continuous Monitoring Plan
- Breach Recovery Plan
- Automation
- MEP Involvement at the National and State Level
- Penetration Testing – UpTech Services, Shelbyville Tech
- Continuous evaluation of risk (threats, vulnerabilities…)
- Participation in Y-12, Man Tech, Securing American Manufacturing Program
- Security Technology Projects – Blockchain

Future Challenges and Direction

- **Flow Down / Supply-chain accountability**
- **Need built-in incentives to maintain strong cyber posture**
- **Growing Cyber Threats – *(Spear Fishing 80%)***
- **Cloud Services Considerations**



create_ ometricsTables create_COITables create_CSTables create_CTATables create_DCGSDocsTables create_DomexTables create_EvRTables create_FacetingTables create_HLTTables create_ISTTables create_KoverseTables create_NGramTables

create_ nopticonTables create_provenanceTables create_RBACTables create_RTRGTables create_SRLTables create_STMTables create_SynthesysTables create_UCDTables drop_BiometricsTables drop_COITables drop_CSTables drop_CTATables

drop_ CGSDocsTables drop_DomexTables drop_EvRTables drop_FacetingTables drop_HLTTables drop_ISTTables drop_KoverseTables drop_NGramTables drop_panopticonTables drop_provenanceTables drop_RBACTables drop_RTRGTables

drop_ RLTables drop_STMTables drop_SynthesysTables drop_UCDTables grant_BiometricsTables grant_COITables grant_CSTables grant_CTATables grant_DCGSDocsTables grant_DomexTables grant_EvRTables grant_FacetingTables

grant_ LTTables grant_ISTTables grant_KoverseTables grant_NGramTables grant_panopticonTables grant_provenanceTables grant_RBACTables grant_RTRGTables grant_SRLTables grant_STMTables grant_SynthesysTables grant_UCDTables

p_create_ rant_all_ iep_create_users_all iep_drop_all.sh iep_rename_all. README rename_BiometricsT rename_COITables rename_CSTables rename_CTATables rename_DCGSDocsT rename_DomexTabl rename_EvRTables

Questions?