

Addressing data collection management challenges: Ensuring data collection software meets FISMA Security Standards

Craig R. Hollingsworth



FedCASIC Conference

April 2022

The Problem

- Federal clients focusing on security
- Documentation requirements are increasingly enforced
- Federal FISMA standards help ensure data collection instruments are secure
- Assure the government agency that data collected on their behalf remains secure

The Problem - Continued

- Legacy projects are also being examined and required to complete the ***Security Authorization and Authority to Operate (ATO)*** process
- How to help the transition
- RTI Document Repository developed with samples and references
 - Bill Savage
 - Keith Wurst
- Web resources

Authority to Operate (ATO) Process

- Security Authorization process to receive an Authority to Operate (ATO)
- Each client has a different set of templates – all based on National Institute of Standards and Technology (NIST) 800-53 and associated documents
- Process is iterative
- Project must complete the client documentation templates
- Iterations until client okays the overall package

Overview

- New projects fielded by RTI are requiring more complete documentation of the IT system in use
 - *Example: New projects are often accompanied by a zip file of 6 -14 documents that may be required*
- Legacy projects are also now being tagged by federal agency security teams
 - *Example: - Three legacy projects went from a two-page security document to a package of templates – one included 15 template docs*

Overview

- Projects now are being required to complete the Security Authorization process to receive an Authority to Operate (ATO)
 - *Example: - Three legacy projects in production for 6-10 years were tapped to complete the documents and achieve an ATO*

ATO Process – Sample Template Package

- A military client directed our team to the **I-Assure website** for document templates
- In line with the NIST Special Publication 800-53 guidelines for selecting and specifying security controls and assessment procedures to verify compliance.

The documentation offered:

- Consistent, comparable, and repeatable approach to evaluating controls
- Stable, yet flexible documentation format
- Individual traceability
- Foundation for the development of additional documents

ATO Process Documents– I-Assure Risk Management Framework



AC – Access Control

1 file(s) 15252 downloads



AT – Awareness and Training

1 file(s) 10561 downloads



AU – Audit and Accountability

1 file(s) 10791 downloads



CA – Security Assessment and Authorization

1 file(s) 10247 downloads



CM – Configuration Management

1 file(s) 10736 downloads



CP – Contingency Planning

1 file(s) 10155 downloads



IA – Identification and Authentication

1 file(s) 9708 downloads



IR – Incident Response

1 file(s) 10679 downloads



MA – Maintenance

1 file(s) 9476 downloads



MP – Media Protection

1 file(s) 9296 downloads



PE – Physical and Environmental Protection

1 file(s) 8987 downloads



PL – Planning

1 file(s) 9448 downloads



PM – Program Management

1 file(s) 9506 downloads



PS – Personnel Security

1 file(s) 9497 downloads



RA – Risk Assessment

1 file(s) 10180 downloads



SA – System and Services Acquisition

1 file(s) 9412 downloads



SC – System and Communications Protection

1 file(s) 9815 downloads



SI – System and Information Integrity

1 file(s) 9933 downloads

ATO Process – Sample Security Document – Contingency Planning

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix I, "Detailed Compliance Matrix"](#).

CNTL-NO.	CONTROL-NAME	PRIORITY	LOW	MOD	HIGH
CP-1	Contingency-Planning-Policy-and-Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency-Plan	P1	CP-2	CP-2-(1)-(3)-(8)	CP-2-(1)-(2)-(3)-(4)-(5)-(8)
CP-3	Contingency-Training	P2	CP-3	CP-3	CP-3-(1)
CP-4	Contingency-Plan-Testing	P2	CP-4	CP-4-(1)	CP-4-(1)-(2)
CP-5	Contingency-Plan-Updates	N/A	Not-Selected	Not-Selected	Not-Selected
CP-6	Alternate-Storage-Site	P1	Not-Selected	CP-6-(1)-(3)	CP-6-(1)-(2)-(3)
CP-7	Alternate-Processing-Site	P1	Not-Selected	CP-7-(1)-(2)-(3)	CP-7-(1)-(2)-(3)-(4)
CP-8	Telecommunications-Services	P1	Not-Selected	CP-8-(1)-(2)	CP-8-(1)-(2)-(3)-(4)

FOR-OFFICIAL-USE-ONLY

FOR-OFFICIAL-USE-ONLY

TTBSAPT
INFORMATION-SYSTEMS-CONTINGENCY-PLAN- 1-21-2020

CNTL-NO.	CONTROL-NAME	PRIORITY	LOW	MOD	HIGH
CP-9	Information-System-Backup	P1	CP-9	CP-9-(1)	CP-9-(1)-(2)-(3)-(5)
CP-10	Information-System-Recovery-and-Reconstitution	P1	CP-10	CP-10-(2)	CP-10-(2)-(4)
CP-11	Alternate-Communications-Protocols	P0	Not-Selected	Not-Selected	Not-Selected
CP-12	Safe-Mode	P0	Not-Selected	Not-Selected	Not-Selected
CP-13	Alternative-Security-Mechanisms	P0	Not-Selected	CP-1	CP-1

Table 1--SP-800-53v4-Compliance-Matrix

Authority to Operate (ATO) Process

- Once complete documentation package is assembled, it is submitted to the client agency security analysts for review
- Once review is passed and any questions are addressed, the Chief Information Officer or designate will sign the ATO letter
- Ultimate Goal - Gives the project the OK to go ahead and open the system to the internet for data collection or other functions

Health and Human Services (HHS) Templates for CDC Projects

CDC Home



Centers for Disease Control and Prevention

CDC 24/7: Saving Lives. Protecting People.™

SEARCH

A-Z Index [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#) <#>

CDC Unified Process

[Management Guide](#)

[Practices](#)

[Templates](#)

[Checklists](#)

[Document Library](#)

[Newsletter](#)

[Contact UP](#)

UP Hot Spot

A Work Breakdown Structure (WBS) defines the what of a project and the project schedule defines the When and Who of a project.

Templates



This web page is archived for historical purposes and is no longer being updated. Please go to CDC Home or use the A-Z Index or Search for more recent information.






















CDC UP Templates are standardized project management documents that project teams can use as a starting point for their project management documents, customizing them to meet the unique needs of each project. Each template includes content commonly used in such a document, boilerplate text, and instructions to the author to assist them in completing and adapting the template for use on their project. CDC UP templates are provided as guidance to be used in the absence of something more sophisticated already available to the project team.

Socialize the CDC Unified Process:

Document Name	Area	Phase
Acquisition Strategy *	Procurement	Implementation
Annual Operational Analysis *	Quality	Operation
Business Case *	Scope	Concept
Business Case LITE	Scope	Concept
Business Impact Analysis	Scope	Implementation
Business Need Statement	Scope	Initiation
Capacity Planning	Risk	Design
Certification and Accreditation Process Templates	Risk	As Needed
Change Management Log	Integration	As Needed
Change Management Plan	Quality	Concept

CDC Templates

<https://www2a.cdc.gov/cdcup/library/templates/default.htm>

 Project Completion (Close-Out/Archive)	Integration	Disposition
 Project Kick-Off Meeting	Communication	Concept
 Project Management Plan	Integration	Planning
 Project Management Plan LITE	Integration	Planning
 Project Process Agreement	Integration	Planning
 Project Schedule (.mpp)	Time	Concept
 Project Schedule (.xls)	Time	Concept
 Project Schedule - Agile (.mpp)	Time	Concept
 Project Schedule - Agile Backlog (.mpp)	Time	Concept
 Quality Management Plan	Integration	Concept
 Quality Management Plan LITE	Integration	Concept
 Release Strategy *	Quality	Concept
 Requirements Definition (functional)	Quality	Concept
 Requirements Definition (non-functional)	Scope	Concept
 Requirements Management Plan	Scope	Concept
 Requirements Traceability Matrix	Scope	Concept
 Risk Management Log	Risk	As Needed
 Risk Management Plan	Risk	Concept
 Risk Management Plan LITE	Risk	Concept
 Service Level Agreement / Memorandum of Understanding *	Communication	Implementation
 Security Approach *	Risk	Concept

ATO Process – Federal Agency Sample of new process – contractor as vendor

<<Insert name>> SYSTEM SECURITY PLAN	Last Updated: <<Insert date>>										
1. SYSTEM IDENTIFICATION											
1.1. System Name/Title: [State the name of the system. Spell out acronyms.]											
1.1.1. System Categorization: Moderate Impact for Confidentiality											
1.1.2. System Unique Identifier: [Insert the System Unique Identifier]											
1.2. Responsible Organization:											
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 20%;">Name:</td><td></td></tr> <tr><td>Address:</td><td></td></tr> <tr><td>Phone:</td><td></td></tr> </table>		Name:		Address:		Phone:					
Name:											
Address:											
Phone:											
1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI):											
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 20%;">Name:</td><td></td></tr> <tr><td>Title:</td><td></td></tr> <tr><td>Office Address:</td><td></td></tr> <tr><td>Work Phone:</td><td></td></tr> <tr><td>e-Mail Address:</td><td></td></tr> </table>		Name:		Title:		Office Address:		Work Phone:		e-Mail Address:	
Name:											
Title:											
Office Address:											
Work Phone:											
e-Mail Address:											
1.2.1.1. System Owner (assignment of security responsibility):											
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 20%;">Name:</td><td></td></tr> <tr><td>Title:</td><td></td></tr> <tr><td>Office Address:</td><td></td></tr> <tr><td>Work Phone:</td><td></td></tr> <tr><td>e-Mail Address:</td><td></td></tr> </table>		Name:		Title:		Office Address:		Work Phone:		e-Mail Address:	
Name:											
Title:											
Office Address:											
Work Phone:											
e-Mail Address:											
1.2.1.2. System Security Officer:											
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 20%;">Name:</td><td></td></tr> <tr><td>Title:</td><td></td></tr> <tr><td>Office Address:</td><td></td></tr> <tr><td>Work Phone:</td><td></td></tr> <tr><td>e-Mail Address:</td><td></td></tr> </table>		Name:		Title:		Office Address:		Work Phone:		e-Mail Address:	
Name:											
Title:											
Office Address:											
Work Phone:											
e-Mail Address:											
1.3. General Description/Purpose of System: What is the function/purpose of the system? [Provide a short, high-level description of the function/purpose of the system.]											
1.3.1. Number of end users and privileged users: [In the table below, provide the approximate number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]											

ATO Process – Federal Agency Sample of new process

<<Insert name>> SYSTEM SECURITY PLAN Last Updated: <<Insert date>>

3.1. Access Control

3.1.1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

Implemented Planned to be Implemented Not Applicable
Current implementation or planned implementation details. If “Not Applicable,” provide rationale.

3.1.2. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

Implemented Planned to be Implemented Not Applicable
Current implementation or planned implementation details. If “Not Applicable,” provide rationale.

3.1.3. Control the flow of CUI in accordance with approved authorizations.





























Implemented Planned to be Implemented Not Applicable
Current implementation or planned implementation details. If “Not Applicable,” provide rationale.

3.1.4. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Implemented Planned to be Implemented Not Applicable
Current implementation or planned implementation details. If “Not Applicable,” provide rationale.

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

ATO Process – Federal Agency Sample

 Business Impact AnalysisTemplate	
 Configuration Management Plan Template	
 Contingency Plan Template	
 Contingency Test Report Template	
 E-Auth_Template	
 Incident Response Plan (IRP) Template, 2018-02-13	
 ISA Template	
 MOU Template	
 POA&M Template	
 Privacy Impact Assessment Template	
 Security Assessment Report (Risk Assessment Report) Template	
 System Inventory Submission Workbook - Final	
 System Security Plan Template, Low, SP800-53 Rev 4	
 System Security Plan Template, Moderate, SP800-53 Rev 4	

To Assist the ATO Process

- RTI developed a repository and website for digitized security documentation
- Bill Savage, Keith Wurst, myself
- Can be searched through metadata tagging

RTI Data Security Repository Overview

- **Benefits:**

- A user-friendly tool for guidance, templates, and examples
- Contains information on the Authority to Operate (ATO) and Security Assessment and Authorization (SA&A) processes
- Make available template documents, proposal text, and other artifacts
- Help create an Institute-wide awareness of data security and the burgeoning federal requirements

Landing Page – Data Security Repository

Developer Resources › Data Security Repository

Data Security Repository

The Data Security Repository is a tool that provides Security information and guidance for staff who need to understand security requirements or produce security materials for developing proposals or performing project activities.

The repository is available to help staff review examples and acquire ready-to-use material that can be tailored to their specific situation. Material within the repository is commonly used for supporting the Security Assessment and Authorization (SA&A), or Certification and Accreditation (C&A), process. This is the process of testing and evaluating the technical and nontechnical security features of an IT system to determine its compliance with a set of specified security requirements in order to obtain an Authority to Operate (ATO) decision.

Access the repository using this link: [Data Security Repository](#).

Browse or Guided Access

Developer Resources > Data Security Repository

Welcome, Craig Hollingsworth

Data Security Repository

Welcome to the RCD Digital Security Repository.

The repository holds a growing collection of security-related documents. The documents are described and categorized across multiple characteristics to help users locate documents that are related to their needs.

This site provides two ways to access documents. You can Browse the entire collection of documents in the repository using simple selection criteria or use a Guided Access interface to help locate appropriate documents more quickly. Select Browse to specify selection criteria to identify documents. Select Guided Access to determine the set of documents that most closely matches your situation. You will be able to view information about documents that match your criteria and download them if desired.

[Browse Materials](#)

[Guided Access](#)

Browse Materials

Developer Resources

- > Repository Home
- > **Browse Materials**
- > Guided Access
- > Admin
- > Logout

Developer Resources > Data Security Repository

Welcome, Craig Hollingsworth

Data Security Repository

Browse Materials

Select from the options below or leave each selection blank and click **View Documents** to see all unfiltered results.

Select Entity... ▼

Select FIPS Rating... ▼

Select Text or Budget... ▼

Select Document Type... ▼

Keywords

View Documents

Browse results – no input

Developer Resources > Data Security Repository Welcome, Craig Hollingsworth

Data Security Repository

Browse Materials

Results Criteria Search Again

Summary ▲	Key Words ▼
ACF Designation of System Owner memo	System, Owner
ACF PIA/PTA Writers Handbook	PTA, PIA, Privacy, Threshold, Impact, Handbook
ACF PTA template	PTA, Privacy, Threshold, Assessment
ACF System Registration form	System, Registration
AHRQ E-Auth template.	E-Auth
AHRQ Incident Response Plan template.	IRP, Incident, Response
AHRQ POA&M template.	POA&M, POAM, Actions, Milestones
AHRQ System Inventory Submission Workbook template.	Inventory, Assets

Search Results

Data Security Repository

[Browse Materials](#)

Document Category: Doc

Subcategory: Project

Summary: AHRQ Incident Response Plan template.

Notes: Incident response plan to respond to computer security incidents.

[Download File](#)

Template: Yes

Filename: [rca_sr_ahrq_incident_response_plan_template.docx](#)

File Version:

File Format: Word

Staff Source:

Source Date: 3/19/2021

Author:

Entity: AHRQ

Status: Final

Project:

Proposal:

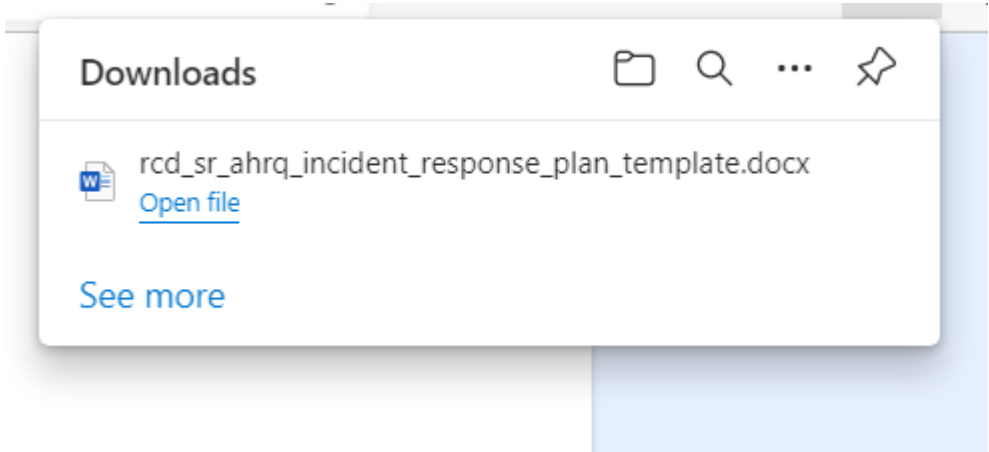
FIPS:

FISMA: Yes

NIST: Yes

SAA: Yes

Download a template



IR Plan Template

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

1.0	→ INCIDENT HANDLING PROCESS.....	4
1.1	→ AUTHORITY	7
1.2	→ SYSTEM DESCRIPTION	8
1.3	→ COMPUTER SECURITY INCIDENTS	10
1.4	→ PURPOSE AND SCOPE	10
1.5	→ AUDIENCE	11
1.6	→ BACKGROUND	11
2.0	→ INCIDENT RESPONSE TEAM	13
2.1	→ TEAM ROLES AND RESPONSIBILITIES	13
3.0	→ HANDLING AN INCIDENT	15
3.1	→ PROCESS OVERVIEW	15
3.2	→ PREPARATION	18
3.3	→ PREVENTION	19
3.4	→ IDENTIFICATION	19
3.5	→ CONTAINMENT	19
3.6	→ ERADICATION	19
3.7	→ RECOVERY	20
4.0	→ POST-INCIDENT ACTIVITY	21
4.1	→ LESSONS LEARNED MEETING	21
4.2	→ DOCUMENTATION	21
4.3	→ PRESERVING EVIDENCE	22
4.4	→ INFORMATION SHARING	22
APPENDIX A: CONTACT LIST		23
2. Reporting a Suspected or Confirmed PII Breach		23
APPENDIX B: SPARS SECURITY INCIDENT REPORTING DOCUMENT		25
APPENDIX B: AFTER ACTION REPORT TEMPLATE		26

Online Resources



- <https://i-assure.com/download-category/rmf-templates/>.
- HHS – CDC/ Templates
<https://www2a.cdc.gov/cdcup/library/templates/default.htm>



Thank you

Contact: Craig Hollingsworth | email: crh@rti.org