Control Implementation Summary (CIS) Template



<Vendor Name>

<Information System Name>

<Sensitivity Level>

Version 1.0

May 2, 2012

**Company Sensitive and Proprietary**

**For Authorized Use Only**

nistBlue

Table of Contents

ABOUT THIS DOCUMENT 4

Who should use this document? 4

Conventions used in this document 4

How to contact us 5

1. INTRODUCTION 5

1.1. Purpose 5

1.2. Scope 5

1.3. System Description 6

2. CONTROL IMPLEMENTATION RESULTS 7

APPENDIX A.   ACRONYMS 9

APPENDIX B.   REFERENCES 10

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version | Author |
| 05/02/2012 | Document Publication | 1.0 | FedRAMP Office |
|  |  |  |  |
|  |  |  |  |

ABOUT THIS DOCUMENT

This document is released in template format. Once populated with content, this document will include detailed information about service provider information security controls.

Who should use this document?

This document is intended to be used by Cloud Service Providers (CSPs) who are applying for an Authorization to Operate (ATO) through the U.S. federal government FedRAMP program.

This template provides a sample format for preparing the Control Implementation Summary (CIS) Report for the CSP information system. The CSP may modify the format as necessary to comply with its internal policies and Federal Risk and Authorization Management Program (FedRAMP) requirements.

Conventions used in this document

This document uses the following typographical conventions:

*Italic*

Italics are used for email addresses, security control assignments parameters, and formal document names.

*Italic blue in a box*

Italic blue text in a blue box indicates instructions to the individual filling out the template.

*Instruction: This is an instruction to the individual filling out of the template.*

**Bold**

Bold text indicates a parameter or an additional requirement.

Constant width

Constant width text is used for text that is representative of characters that would show up on a computer screen.

<**Brackets**>

Bold blue text brackets indicate a user defined variable or word that should be replaced with a specific name. Once replaced, the brackets should be removed.

Notes

Notes are found between parallel lines and include additional information that may be helpful to the users of this template.

**Note:** This is a note.

Sans Serif

Sans Serif text is used for tables, table captions, figure captions, and table of contents.

Sans Serif Gray

Sans Serif gray text is used for examples.

How to contact us

If you have questions about something in this document, or how to fill it out, please write to:

info@fedramp.gov

For more information about the FedRAMP project, please see the website at:

<http://www.fedramp.gov>

1. INTRODUCTION

The Control Implementation Summary (CIS) report is a key document in the security authorization package developed for submission to the Federal Risk and Authorization Management Program (FedRAMP) authorizing officials. The CIS report includes control implementation responsibility and implementation status of the FedRAMP security controls. CIS along with the Control Tailoring Workbook (CTW) and FIPS-199 Security Categorization should be submitted and approved by FedRAMP JAB before submitting the System Security Plan (SSP).

* 1. Purpose

The purpose of the Control Implementation Summary (CIS) is to delineate the control responsibilities of CSPs and customer agencies. In addition, the CIS provides a summary of all required controls and enhancements across the system. CSPs are requested to coordinate with their assigned FedRAMP ISSO to ensure the CIS is appropriately formatted to reflect status and control origination responsibilities.

* 1. Scope

The scope of the CIS template includes a description of all management, operational, and technical FedRAMP security controls that will be documented in the security plan (SP) at the determined impact level (Moderate or Low) by the CSP.

* 1. System Description

The ***<*Information System Name*>***system has been determined to have a security categorization of <**Moderate/Low**>.

*Instruction: Insert a brief high-level description of the system, business or purpose and system environment. Ensure this section is continuously updated with the latest description from the System Security Plan (SSP).*

1. CONTROL IMPLEMENTATION RESULTS

Columns in the embedded Control Implementation Summary (CIS) spreadsheet are defined according to the definitions found in the table that follows.

| **Control Origination** | **Definition** | **Example** |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the CSP corporate network. | DNS from the corporate network provides address resolution services for the information system and the service offering. |
| Service Provider System Specific | A control specific to a particular system at the CSP and the control is not part of the service provider corporate controls. | A unique host based intrusion detection system (HIDs) is available on the service offering platform but is not available on the corporate network. |
| Service Provider Hybrid | A control that makes use of both corporate controls and additional controls specific to a particular system at the CSP. | Scans of the corporate network infrastructure; scans of databases and web based application are system specific. |
| Configured by Customer | A control where the customer needs to apply a configuration in order to meet the control requirement. | User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc.), entering an IP range specific to their organization are configurable by the customer. |
| Provided by Customer | A control where the customer needs to provide additional hardware or software in order to meet the control requirement. | The customer provides a SAML SSO solution to implement two-factor authentication. |
| Shared | A control that is managed and implemented partially by the CSP and partially by the customer. | Security awareness training must be conducted by both the CSP and the customer. |
| Inherited from pre-existing Provisional Authorization | A control that is inherited from another CSP system that has already received a Provisional Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

*Instruction: The CSP should indicate the control implementation status and control implementation origination of each of the controls identified in the CIS workbook by providing a checkmark in the appropriate cell. For the controls and enhancements identified as being a shared control, the CSP should explain the customer configuration and/or implementation responsibility in the “Customer Responsibility Matrix” which is on the second sheet in the workbook. The CIS should be entirely consistent with the Control Summary Information tables found in the System Security Plan.*

Embedded CIS Spreadsheet (Click to open):



APPENDIX A.   ACRONYMS

*Instruction: Update the acronyms based on the acronyms used in this document.*

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| AC | Authentication Category |
| AP  API | Assurance Profile  Application Programming Interface |
| ATO | Authorization to Operate |
| C&A | Certification & Accreditation |
| COTS | Commercial Off the Shelf |
| AO  FedRAMP | Authorizing Official  Federal Risk and Authorization Management Program |
| FIPS PUB | Federal Information Processing Standard Publication |
| FISMA | Federal Information Security Management Act |
| GSS  IaaS | General Support System  Infrastructure as a Service (Model) |
| IATO | Interim Authorization to Operate |
| ID | Identification |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST | National Institute of Standards and Technology |
| OMB | Office of Management and Budget |
| PIA | Privacy Impact Assessment |
| POA&M | Plan of Action and Milestones |
| POC | Point of Contact |
| RA  Rev. | Risk Assessment  Revision |
| SA | Security Assessment |
| SAR | Security Assessment Report |
| SDLC | System Development Life Cycle |
| SP | Special Publication |
| SSP  VLAN | System Security Plan  Virtual Local Area Network |

APPENDIX B.   REFERENCES

Laws and Regulations:

* Federal Information Security Management Act of 2002, Title III – Information Security, P.L. 107-347.
* Consolidated Appropriations Act of 2005, Section 522.
* USA PATRIOT Act (P.L. 107-56), October 2001.

OMB Circulars:

* OMB Circular A-130, Management of Federal Information Resources, November 2000.
* OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005.
* OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June, 2006.

FIPS Publications:

* FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
* FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
* FIPS PUB 201, Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST Publications:

* NIST 800-18 Revision 1 Guide for Developing Security Plans for Information Technology Systems
* NIST 800-30, Risk Management Guide for Information Technology Systems
* NIST 800-34, Contingency Planning Guide for Information Technology Systems
* NIST 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
* NIST 800-47, Security Guide for Interconnecting Information Technology Systems
* NIST 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations
* NIST 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information System and Organizations
* NIST 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security
* NIST 800-63, Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology
* NIST 800-64, Security Considerations in the Information System Development Life Cycle