FIPS 199 Categorization (Template)

<Vendor>

<Information System Name>
Version 1.0

May 2, 2012

Company Sensitive and Proprietary
For Authorized Use Only

Table of Contents

List of Tables

Document Revision History

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

ABOUT THIS DOCUMENT

This document has been originally 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 service providers who are applying for a Provisional Authorization through the U.S. federal government FedRAMP program.

This template provides a sample format for preparing a FIPS 199 Categorization Report for the Cloud Service Provider (CSP) information systems. The template follows guidance as set forth in NIST Special Publication 800-60 Volume 2 Revision 1, and is intended to be used as a guide. Modify the format as necessary to comply with your 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>

Text in brackets indicates a generic default name 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 Federal Information Processing Standard 199 (FIPS-199) Categorization (Security Categorization) 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 FIPS-199 Categorization report includes the determination of the security impact level for the cloud environment that may host any or all of the service models (Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The ultimate goal of the security categorization is for the cloud service provider (CSP) to be able to select and implement the FedRAMP security controls applicable to its environment.

1.1. Purpose

The purpose of the FIPS-199 Categorization template is for the CSP to assess and complete the categorization of their cloud environment, to provide the categorization to the System Owner/Certifier and the FedRAMP Joint Authorization Board (JAB) and in helping them to make a determination of the CSP's ability to host systems at that level. The completed security categorization template will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

1.2. Scope

The scope of the FIPS-199 Categorization template includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume 2 Revision 1 document.

1.3. 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, the system environment and the purpose of the system. The description should be consistent with the description found in the System Security Plan (SSP).*

2. METHODOLOGY

Instruction: The CSP should review the NIST Special Publication 800-60 Volume 2 Revision 1 Appendix C Management and Support Information and Information System Impact Levels and Appendix D Impact Determination for Mission-Based Information and Information Systems to assess the recommended impact level for each of the information types. For more information, CSP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the CSP should fill out Table 1.

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS-199 Categorization is the high watermark for the impact level of all the applicable information types.

The FIPS 199 analysis represents the information type and sensitivity levels of the CSP's cloud service offering (and is not intended to include sensitivity levels of agency data). Customer agencies will be expected to perform a separate FIPS 199 analysis for their own data hosted on the CSP's cloud environment. Customers using the CSP cloud environment must ensure that the security categorization of information types collected, processed, or stored on the CSP cloud environment does not exceed the high-water mark of Moderate for confidentiality, integrity, and availability. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

The FedRAMP system CSP categorization is expected to resolve to Moderate or Low.

Instruction: In the first three columns, put the NIST SP-60 V2 R1 recommended impact level. In the next three columns, put in the CSP determined recommended impact level. If the CSP determined recommended impact level does not match the level recommended by NIST, put in an explanation in the last column as to why this decision was made.

Table 1: CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1

Information Type	NIST SP 800-60 V2 R1 Recommended Confidentiality Impact Level	NIST SP 800-60 V2 R1 Recommended Integrity Impact Level	NIST SP 800-60 V2 R1 Recommended Availability Impact Level	CSP Selected Confidentiality Impact Level	CSP Selected Integrity Impact Level	CSP Selected Availability Impact Level	Statement for Impact Adjustment Justification

APPENDIX A. ACRONYMS

Acronyms	Definition
AC	Authentication Category
AP	Assurance Profile
API	Application Programming Interface
ATO	Authorization to Operate
C&A	Certification & Accreditation
COTS	Commercial Off the Shelf
AO	Authorizing Official
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Management Act
GSS	General Support System
IaaS	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	Risk Assessment
R1	Revision 1
SA	Security Assessment
SAR	Security Assessment Report
SDLC	System Development Life Cycle
SP	Special Publication
SSP	System Security Plan
VLAN	Virtual Local Area Network

APPENDIX B. REFERENCES

Instruction: Update the below list of references to reflect current guidance.

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, Guide for Developing Security Plans for Information Technology Systems
- NIST 800-26, Security Self-Assessment Guide 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, 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 Rev3, Recommended Security Controls for Federal Information Systems and Organizations
- NIST 800-53A Rev1, Guide for Assessing the Security Controls in Federal Information System and Organizations
- NIST 800-60 Rev1, 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