|  |
| --- |
| Fathya Maboune Information Tech Group (PITG) Cloud IaaS System Security Plan (SSP) LOW Baseline  Pendeme Information Technology Group  GDIT Cloud IaaS  Version 3.5  Oscal Version 1.0-Milestone2  Version Date 9/18/2018 |



Instruction: This template contains a number of features to facilitate data entry. As you go through the template entering data, you will see prompts for you to enter different types of data.

Repeatable Field

Some multiple-occurring data fields have been linked together and you need only enter the data once. Enter the data once; then click outside the data entry field and all occurrences of that field will be populated. For example, when you see “Information System Abbreviation” and replace it with your system abbreviation, all instances of the abbreviation throughout the document will be replaced with the value you entered. This document contains the following repeatable fields:

CSP Name

Information System Name

Version Number

Version Date

Information System Abbreviation

If you find a data field from the above list that has not populated, then press the F9 key to refresh the data. If you make a change to one of the above data fields, you may also have to press the F9 key to refresh the data throughout the document. Remember to save the document after refreshes. The one exception to the repeatable fields is information system names for FedRAMP or leveraged authorizations that are identified as “Leveraged information system name:

Date Selection

Data fields that must contain a date will present a date selection menu.

Item Choice

Data fields that have a limited number of value choices will present a selection list.

Number Entry

Data fields that must have numeric values display “number.”

Text Entry

Many data fields, particularly in tables, that can contain any text display “Enter text” or “Click here to enter text.”

Delete this instruction from your final version of this document.

System Security Plan

Prepared by

|  |  |  |
| --- | --- | --- |
| **Identification of Organization that Prepared this Document** | | |
|  | Organization Name | Pendeme Information Technology Group |
| Street Address | 3060 Williams Drive |
| Suite/Room/Building | Suite 100 |
| City, State Zip | Sherbrooke Quebec 22031 |

Prepared for

|  |  |  |
| --- | --- | --- |
| **Identification of Cloud Service Provider** | | |
|  | Organization Name | Security Analysts Corp |
| Street Address | 3060 Williams Drive |
| Suite/Room/Building | Suite 100 |
| City, State Zip | Fairfax VA 22031 |

Te mplate Revision History

|  |  |
| --- | --- |
| **Date** | **Description** |
| 9/18/2018 | Original publication |
| 10/21/2016 | Removed tables in Sec 15.12 FedRAMP Laws and Regulations  Removed revision history tables in all of Sec 15  Removed Acronyms - see FedRAMP Master Acronyms and Glossary resource document  Added PTA to Sec 15.4 PTA and PIA  Added E-Authentication to Sec 15.3  Added FIPs to Sec 15.10 FIPS 199  Changed Inventory instruction and guidance Sec 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 3/6/2017 | Renamed document from "FedRAMP System Security Plan (SSP) Low Baseline Master Template to "FedRAMP System Security Plan (SSP) Low Baseline Template" |
| 6/6/2017 | Updated logo |
| 8/28/2018 | Revised controls for language consistency, updated section 2.3 and Attachment 3, added guidance to SA -9, updated requirements in RA-5 |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version of SSP | Author |
| 9/18/2018 | <Revision Description> | <Version> | <Author> |
| 9/18/2018 | <Revision Description> | <Version> | <Author> |
| 9/18/2018 | <Revision Description> | <Version> | <Author> |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact [*info@FedRAMP.gov*](mailto:info@fedramp.gov)

For more information about the FedRAMP project, see [www.FedRAMP.gov](http://www.fedramp.gov)

Instruction: The System Security Plan is the main document in which the Cloud Service Provider (CSP) describes all the security controls in use on the information system and their implementation.

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

This document is intended to be used by service providers who are applying for a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) or an Agency Authorization to Operate (ATO) through the Federal Risk and Authorization Management Program (FedRAMP).  
  
In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Note that “-1” Controls (AC-1, AU-1, SC-1, etc.)\* cannot be inherited and must be described in some way by the service provider.  
\*Access Control (AC), Audit and Accountability (AU), System and Communications Protection (SC)

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For System as a Service (SaaS) and Platform as a Service (PaaS) systems that are inheriting controls from an Infrastructure as a Service (IaaS) (or anything lower in the stack), the “inherited” check box must be checked and the implementation description must simply say “inherited.” FedRAMP reviewers will determine whether the control-set is appropriate or not.

In Section 13, the National Institute of Standards and Technology (NIST) term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases, the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.

Delete this instruction from your final version of this document.

TABLE OF CONTENTS

[1. Information System Name/Title 1](#_Toc523078834)

[2. Information System Categorization 1](#_Toc523078835)

[2.1. Information Types 1](#_Toc523078836)

[2.2. Security Objectives Categorization (FIPS 199) 3](#_Toc523078837)

[2.3. Digital Identity Determination 4](#_Toc523078838)

[3. Information System Owner 4](#_Toc523078839)

[4. Authorizing Official 4](#_Toc523078840)

[5. Other Designated Contacts 5](#_Toc523078841)

[6. Assignment of Security Responsibility 6](#_Toc523078842)

[7. Information System Operational Status 7](#_Toc523078843)

[8. Information System Type 7](#_Toc523078844)

[8.1. Cloud Service Models 7](#_Toc523078845)

[8.2. Cloud Deployment Models 8](#_Toc523078846)

[8.3. Leveraged Authorizations 9](#_Toc523078847)

[9. General System Description 9](#_Toc523078848)

[9.1. System Function or Purpose 9](#_Toc523078849)

[9.2. Information System Components and Boundaries 9](#_Toc523078850)

[9.3. Types of Users 10](#_Toc523078851)

[9.4. Network Architecture 11](#_Toc523078852)

[10. System Environment And Inventory 12](#_Toc523078853)

[10.1. Data Flow 13](#_Toc523078854)

[10.2. Ports, Protocols and Services 14](#_Toc523078855)

[11. System Interconnections 15](#_Toc523078856)

[12. Laws, Regulations, Standards and Guidance 17](#_Toc523078857)

[12.1. Applicable Laws and Regulations 17](#_Toc523078858)

[12.2. Applicable Standards and Guidance 17](#_Toc523078859)

[13. Minimum Security Controls 18](#_Toc523078860)

[13.1. Access Control (AC) 26](#_Toc523078861)

[AC-1 Access Control Policy and Procedures Requirements (L) (M) 26](#_Toc523078862)

[AC-2 Account Management (L) (M) 27](#_Toc523078863)

[AC-3 Access Enforcement (L) (M) (H) 28](#_Toc523078864)

[AC-7 Unsuccessful Login Attempts (L) (M) 29](#_Toc523078865)

[AC-8 System Use Notification (L) (M) (H) 30](#_Toc523078866)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 33](#_Toc523078867)

[AC-17 Remote Access (L) (M) (H) 33](#_Toc523078868)

[AC-18 Wireless Access Restrictions (L) (M) (H) 34](#_Toc523078869)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 35](#_Toc523078870)

[AC-20 Use of External Information Systems (L) (M) (H) 36](#_Toc523078871)

[AC-22 Publicly Accessible Content (L) (M) (H) 37](#_Toc523078872)

[13.2. Awareness and Training (AT) 38](#_Toc523078873)

[AT-1 Security Awareness and Training Policy and Procedures (L) (M) 38](#_Toc523078874)

[AT-2 Security Awareness (L) (M) (H) 39](#_Toc523078875)

[AT-3 Role-Based Security Training (L) (M) (H) 39](#_Toc523078876)

[AT-4 Security Training Records (L) (M) 40](#_Toc523078877)

[13.3. Audit and Accountability (AU) 41](#_Toc523078878)

[AU-1 Audit and Accountability Policy and Procedures (L) (M) 41](#_Toc523078879)

[AU-2 Audit Events (L) (M) (H) 42](#_Toc523078880)

[AU-3 Content of Audit Records (L) (M) (H) 43](#_Toc523078881)

[AU-4 Audit Storage Capacity (L) (M) (H) 44](#_Toc523078882)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 45](#_Toc523078883)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 45](#_Toc523078884)

[AU-8 Time Stamps (L) (M) (H) 46](#_Toc523078885)

[AU-9 Protection of Audit Information (L) (M) (H) 47](#_Toc523078886)

[AU-11 Audit Record Retention (L) (M) 48](#_Toc523078887)

[AU-12 Audit Generation (L) (M) (H) 49](#_Toc523078888)

[13.4. Security Assessment and Authorization (CA) 50](#_Toc523078889)

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M) 50](#_Toc523078890)

[CA-2 Security Assessments (L) (M) (H) 51](#_Toc523078891)

[CA-2 (1) Control Enhancement (L) (M) (H) 52](#_Toc523078892)

[CA-3 System Interconnections (L) (M) (H) 53](#_Toc523078893)

[CA-5 Plan of Action and Milestones (L) (M) (H) 54](#_Toc523078894)

[CA-6 Security Authorization (L) (M) (H) 55](#_Toc523078895)

[CA-7 Continuous Monitoring (L) (M) (H) 56](#_Toc523078896)

[CA-9 Internal System Connections (L) (M) (H) 58](#_Toc523078897)

[13.5. Configuration Management (CM) 59](#_Toc523078898)

[CM-1 Configuration Management Policies and Procedures (L) (M) 59](#_Toc523078899)

[CM-2 Baseline Configuration (L) (M) (H) 60](#_Toc523078900)

[CM-4 Security Impact Analysis (L) (M) (H) 61](#_Toc523078901)

[CM-6 Configuration Settings (L) (M) (H) 62](#_Toc523078902)

[CM-7 Least Functionality (L) (M) (H) 63](#_Toc523078903)

[CM-8 Information System Component Inventory (L) (M) (H) 64](#_Toc523078904)

[CM-10 Software Usage Restrictions (L) (M) (H) 65](#_Toc523078905)

[CM-11 User-Installed Software (L) (M) (H) 66](#_Toc523078906)

[13.6. Contingency Planning (CP) 67](#_Toc523078907)

[CP-1 Contingency Planning Policy and Procedures (L) (M) 67](#_Toc523078908)

[CP-2 Contingency Plan (L) (M) (H) 68](#_Toc523078909)

[CP-3 Contingency Training (L) (M) (H) 70](#_Toc523078910)

[CP-4 Contingency Plan Testing (L) 71](#_Toc523078911)

[CP-9 Information System Backup (L) (M) (H) 72](#_Toc523078912)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 73](#_Toc523078913)

[13.7. Identification and Authentication (IA) 74](#_Toc523078914)

[IA-1 Identification and Authentication Policy and Procedures (L) (M) 74](#_Toc523078915)

[IA-2 User Identification and Authentication (L) (M) (H) 75](#_Toc523078916)

[IA-2 (1) Control Enhancement (L) (M) (H) 75](#_Toc523078917)

[IA-2 (12) Control Enhancement (L) (M) (H) 76](#_Toc523078918)

[IA-4 Identifier Management (L) (M) 77](#_Toc523078919)

[IA-5 Authenticator Management (L) (M) 78](#_Toc523078920)

[IA-5 (1) Control Enhancement (L) (M) 80](#_Toc523078921)

[IA-5 (11) Control Enhancement (L) (M) (H) 81](#_Toc523078922)

[IA-6 Authenticator Feedback (L) (M) (H) 82](#_Toc523078923)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 82](#_Toc523078924)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 83](#_Toc523078925)

[IA-8 (1) Control Enhancement (L) (M) (H) 84](#_Toc523078926)

[IA-8 (2) Control Enhancement (L) (M) (H) 84](#_Toc523078927)

[IA-8 (3) Control Enhancement (L) (M) (H) 85](#_Toc523078928)

[IA-8 (4) Control Enhancement (L) (M) (H) 85](#_Toc523078929)

[13.8. Incident Response (IR) 86](#_Toc523078930)

[IR-1 Incident Response Policy and Procedures (L) (M) 86](#_Toc523078931)

[IR-2 Incident Response Training (L) (M) 87](#_Toc523078932)

[IR-4 Incident Handling (L) (M) (H) 88](#_Toc523078933)

[IR-5 Incident Monitoring (L) (M) (H) 89](#_Toc523078934)

[IR-6 Incident Reporting (L) (M) (H) 90](#_Toc523078935)

[IR-7 Incident Response Assistance (L) (M) (H) 91](#_Toc523078936)

[IR-8 Incident Response Plan (L) (M) (H) 91](#_Toc523078937)

[13.9. Maintenance (MA) 93](#_Toc523078938)

[MA-1 System Maintenance Policy and Procedures (L) (M) 93](#_Toc523078939)

[MA-2 Controlled Maintenance (L) (M) (H) 94](#_Toc523078940)

[MA-4 Remote Maintenance (L) (M) (H) 95](#_Toc523078941)

[MA-5 Maintenance Personnel (L) (M) (H) 96](#_Toc523078942)

[13.10. Media Protection (MP) 97](#_Toc523078943)

[MP-1 Media Protection Policy and Procedures (L) (M) 97](#_Toc523078944)

[MP-2 Media Access (L) (M) 98](#_Toc523078945)

[MP-6 Media Sanitization and Disposal (L) (M) 99](#_Toc523078946)

[MP-7 Media Use (L) (M) (H) 100](#_Toc523078947)

[13.11. Physical and Environmental Protection (PE) 101](#_Toc523078948)

[PE-1 Physical and Environmental Protection Policy and Procedures (L) (M) 101](#_Toc523078949)

[PE-2 Physical Access Authorizations (L) (M) 102](#_Toc523078950)

[PE-3 Physical Access Control (L) (M) (H) 103](#_Toc523078951)

[PE-6 Monitoring Physical Access (L) (M) (H) 104](#_Toc523078952)

[PE-8 Visitor Access Records (L) (M) (H) 105](#_Toc523078953)

[PE-12 Emergency Lighting (L) (M) (H) 106](#_Toc523078954)

[PE-13 Fire Protection (L) (M) (H) 107](#_Toc523078955)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 107](#_Toc523078956)

[PE-15 Water Damage Protection (L) (M) (H) 108](#_Toc523078957)

[PE-16 Delivery and Removal (L) (M) (H) 109](#_Toc523078958)

[13.12. Planning (PL) 110](#_Toc523078959)

[PL-1 Security Planning Policy and Procedures (L) (M) 110](#_Toc523078960)

[PL-2 System Security Plan (L) (M) (H) 111](#_Toc523078961)

[PL-4 Rules of Behavior (L) (M) 112](#_Toc523078962)

[13.13. Personnel Security (PS) 113](#_Toc523078963)

[PS-1 Personnel Security Policy and Procedures (L) (M) 113](#_Toc523078964)

[PS-2 Position Categorization (L) (M) 114](#_Toc523078965)

[PS-3 Personnel Screening (L) (M) (H) 115](#_Toc523078966)

[PS-4 Personnel Termination (L) (M) 116](#_Toc523078967)

[PS-5 Personnel Transfer (L) (M) 117](#_Toc523078968)

[PS-6 Access Agreements (L) (M) 118](#_Toc523078969)

[PS-7 Third-Party Personnel Security (L) (M) 119](#_Toc523078970)

[PS-8 Personnel Sanctions (L) (M) 120](#_Toc523078971)

[13.14. Risk Assessment (RA) 121](#_Toc523078972)

[RA-1 Risk Assessment Policy and Procedures (L) (M) 121](#_Toc523078973)

[RA-2 Security Categorization (L) (M) (H) 122](#_Toc523078974)

[RA-3 Risk Assessment (L) (M) 123](#_Toc523078975)

[RA-5 Vulnerability Scanning (L) (M) (H) 125](#_Toc523078976)

[13.15. System and Services Acquisition (SA) 126](#_Toc523078977)

[SA-1 System and Services Acquisition Policy and Procedures (L) (M) 126](#_Toc523078978)

[SA-2 Allocation of Resources (L) (M) (H) 127](#_Toc523078979)

[SA-3 System Development Life Cycle (L) (M) (H) 128](#_Toc523078980)

[SA-4 Acquisitions Process (L) (M) (H) 129](#_Toc523078981)

[SA-5 Information System Documentation (L) (M) 130](#_Toc523078982)

[SA-9 External Information System Services (L) (M) (H) 132](#_Toc523078983)

[13.16. System and Communications Protection (SC) 133](#_Toc523078984)

[SC-1 System and Communications Protection Policy and Procedures (L) (M) 133](#_Toc523078985)

[SC-5 Denial of Service Protection (L) (M) (H) 134](#_Toc523078986)

[SC-7 Boundary Protection (L) (M) (H) 135](#_Toc523078987)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 136](#_Toc523078988)

[SC-13 Use of Cryptography (L) (M) (H) 137](#_Toc523078989)

[SC-15 Collaborative Computing Devices (L) (M) (H) 137](#_Toc523078990)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 139](#_Toc523078991)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 140](#_Toc523078992)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 140](#_Toc523078993)

[SC-39 Process Isolation (L) (M) (H) 141](#_Toc523078994)

[13.17. System and Information Integrity (SI) 142](#_Toc523078995)

[SI-1 System and Information Integrity Policy and Procedures (L) (M) 142](#_Toc523078996)

[SI-2 Flaw Remediation (L) (M) (H) 143](#_Toc523078997)

[SI-3 Malicious Code Protection (L) (M) 144](#_Toc523078998)

[SI-4 Information System Monitoring (L) (M) (H) 145](#_Toc523078999)

[SI-5 Security Alerts & Advisories (L) (M) (H) 147](#_Toc523079000)

[SI-12 Information Output Handling and Retention (L) (M) (H) 148](#_Toc523079001)

[SI-16 Memory Protection (L) (M) (H) 148](#_Toc523079002)

[14. Acronyms 150](#_Toc523079003)

[Systems Security Plan Attachments 151](#_Toc523079004)

[15. Attachments 151](#_Toc523079005)

[Attachment 1 Information Security Policies and Procedures 153](#_Toc523079006)

[Attachment 2 User Guide 154](#_Toc523079007)

[Attachment 3 Digital Identity Worksheet 155](#_Toc523079008)

[Introduction and Purpose 155](#_Toc523079009)

[Information System Name/Title 155](#_Toc523079010)

[Digital Identity Level Definitions 155](#_Toc523079011)

[Review Maximum Potential Impact Levels 156](#_Toc523079012)

[Digital Identity Level Selection 157](#_Toc523079013)

[Attachment 4 PTA / PIA 158](#_Toc523079014)

[Privacy Overview and Point of Contact (POC) 158](#_Toc523079015)

[Applicable Laws and Regulations 158](#_Toc523079016)

[Applicable Standards and Guidance 159](#_Toc523079017)

[Personally Identifiable Information (PII) 159](#_Toc523079018)

[Privacy Threshold Analysis 160](#_Toc523079019)

[Qualifying Questions 160](#_Toc523079020)

[Designation 160](#_Toc523079021)

[Attachment 5 Rules of Behavior 161](#_Toc523079022)

[Attachment 6 Information System Contingency Plan 162](#_Toc523079023)

[Attachment 7 Configuration Management Plan 163](#_Toc523079024)

[Attachment 8 Incident Response Plan 164](#_Toc523079025)

[Attachment 9 CIS Workbook 165](#_Toc523079026)

[Attachment 10 FIPS 199 166](#_Toc523079027)

[Introduction and Purpose 166](#_Toc523079028)

[Scope 166](#_Toc523079029)

[System Description 166](#_Toc523079030)

[Methodology 167](#_Toc523079031)

[Attachment 11 Separation of Duties Matrix 169](#_Toc523079032)

[Attachment 12 FedRAMP Laws and Regulations 170](#_Toc523079033)

[Attachment 13 FedRAMP Inventory Workbook 171](#_Toc523079034)

List of Figures

[Figure 9‑1. Authorization Boundary Diagram 10](#_Toc523079035)

[Figure 9‑2. Network Diagram 12](#_Toc523079036)

[Figure 10‑1. Data Flow Diagram 13](#_Toc523079037)

List of Tables

[Table 1‑1. Information System Name and Title 1](#_Toc523079038)

[Table 2‑1. Security Categorization 1](#_Toc523079039)

[Table 2‑2. Sensitivity Categorization of Information Types 3](#_Toc523079040)

[Table 2‑3. Security Impact Level 3](#_Toc523079041)

[Table 2‑4. Baseline Security Configuration 3](#_Toc523079042)

[Table 3‑1. Information System Owner 4](#_Toc523079043)

[Table 5‑1. Information System Management Point of Contact 5](#_Toc523079044)

[Table 5‑2. Information System Technical Point of Contact 5](#_Toc523079045)

[Table 6‑1. CSP Name Internal ISSO (or Equivalent) Point of Contact 6](#_Toc523079046)

[Table 6‑2. AO Point of Contact 6](#_Toc523079047)

[Table 7‑1. System Status 7](#_Toc523079048)

[Table 8‑1. Service Layers Represented in this SSP 8](#_Toc523079049)

[Table 8‑2. Cloud Deployment Model Represented in this SSP 8](#_Toc523079050)

[Table 8‑3. Leveraged Authorizations 9](#_Toc523079051)

[Table 9‑1. Personnel Roles and Privileges 11](#_Toc523079052)

[Table 10‑1. Ports, Protocols and Services 14](#_Toc523079053)

[Table 11‑1. System Interconnections 15](#_Toc523079054)

[Table 12‑1. Information System Name Laws and Regulations 17](#_Toc523079055)

[Table 12‑2. Information System Name Standards and Guidance 17](#_Toc523079056)

[Table 13‑1. Summary of Required Security Controls 18](#_Toc523079057)

[Table 13‑2. Control Origination and Definitions 25](#_Toc523079058)

[Table 13‑3. CA-3 Authorized Connections 53](#_Toc523079059)

[Table 15‑1. Names of Provided Attachments 151](#_Toc523079060)

[Table 15‑2. Information System Name and Title 155](#_Toc523079061)

[Table 15‑3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels 156](#_Toc523079062)

[Table 15‑4. Potential Impacts for Assurance Levels 157](#_Toc523079063)

[Table 15‑5. Digital Identity Level 157](#_Toc523079064)

[Table 15‑6. Information System Name Privacy POC 158](#_Toc523079065)

[Table 15‑7. Information System Name Laws and Regulations 159](#_Toc523079066)

[Table 15‑8. Information System Name Standards and Guidance 159](#_Toc523079067)

[Table 15‑9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 168](#_Toc523079068)

[Table 15‑10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance 170](#_Toc523079069)

System Security Plan Approvals

Cloud Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | Iman Pemy | | Date | **9/18/2018** |
| Title | System Security Plan Approval | | | |
| Cloud Service Provider | | PITG | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Peter Harroun | | Date | **9/18/2018** |
| Title | System Security Plan Approval | | | |
| Cloud Service Provider | | PITG | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Iman Pemy | | Date | **9/18/2018** |
| Title | Information System Owner | | | |
| Cloud Service Provider | | PITG | | |
|  | |  | | |

# Information System Name/Title

This System Security Plan provides an overview of the security requirements for the GDIT Cloud IaaS (GDIT Cloud) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the GDIT Cloud information system.

The security safeguards implemented for the GDIT Cloud system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1‑1. Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1303191948 | GDIT Cloud IaaS | GDIT Cloud |

# Information System Categorization

The overall information system sensitivity categorization is recorded in Table 2‑1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Attachment 10, FIPS 199.**

Table 2‑1. Security Categorization

|  |  |
| --- | --- |
| System Sensitivity Level: | low |

## Information Types

This section describes how the information types used by the information system are categorized for confidentiality, integrity and availability sensitivity levels.

The following tables identify the information types that are input, stored, processed and/or output from GDIT Cloud. The selection of the information types is based on guidance provided by Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office Business Reference Model 2.0 and FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems which is based on NIST Special Publication (SP) 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories.

The tables also identify the security impact levels for confidentiality, integrity and availability for each of the information types expressed as low, moderate, or high. The security impact levels are based on the potential impact definitions for each of the security objectives (i.e., confidentiality, integrity and availability) discussed in NIST SP 800-60 and FIPS Pub 199.

The potential impact is low if—

* The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
* A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is moderate if—

* The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
* A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is high if—

* The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
* A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Instruction: Record your information types in the tables that follow. Record the sensitivity level for Confidentiality, Integrity and Availability as High, Moderate, or Low. Add more rows as needed to add more information types. Use NIST SP 800-60 Guide for Mapping Types of Information and Systems to Security Categories, Volumes I & II, Revision 1 for guidance.

Delete this instruction from your final version of this document.

Example:

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| System Development | C.3.5.1 | Low | Moderate | Low |

Table 2‑2. Sensitivity Categorization of Information Types

| Information Type  (Use only information types from NIST SP 800-60, Volumes I and II  as amended) | NIST 800-60 identifier for Associated Information Type | Confidentiality | Integrity | Availability |
| --- | --- | --- | --- | --- |
| Contingency Planning | C.2.4.1 | fips-199-moderate | fips-199-moderate | fips-199-moderate |
| Continuity of Operations | C.2.4.2 | fips-199-moderate | fips-199-moderate | fips-199-moderate |
| Service Recovery | C.2.4.3 | fips-199-low | fips-199-moderate | fips-199-low |

## Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2‑2. Sensitivity Categorization of Information Types, for the GDIT Cloud, default to the high-water mark for the Information Types as identified in Table 2‑3. Security Impact Level below.

Table 2‑3. Security Impact Level

| Security Objective | Low, Moderate or High |
| --- | --- |
| Confidentiality | fips-199-moderate |
| Integrity | fips-199-moderate |
| Availability | fips-199-moderate |

Through review and analysis, it has been determined that the baseline security categorization for the GDIT Cloud system is listed in the Table 2‑4. Baseline Security Configuration that follows.

Table 2‑4. Baseline Security Configuration

|  |  |
| --- | --- |
| GDIT Cloud Security Categorization | Choose level |

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

## Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

Additional digital identity information can be found in Section 15 Attachments Digital Identity Level Selection.

# Information System Owner

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3‑1. Information System Owner

| Information System Owner Information | |
| --- | --- |
| Name | Iman Pemy |
| Title | Information System Owner |
| Company / Organization | Pendeme Information Technology Group |
| Address | 11400 Westmoor Circle Suite 2501 Westminster CO 80021 US |
| Phone Number | 303-542-8492 |
| Email Address | Matthew.Holcomb@GDIT.com |

# Authorizing Official

Instruction: The Authorizing Official is determined by the path that the CSP is using to obtain an authorization.

JAB P-ATO: FedRAMP, JAB, as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DoD) and Department of Homeland Security (DHS)

Agency Authority to Operate (ATO): Agency Authorizing Official name, title and contact information

Delete this and all other instructions from your final version of this document.

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the Insert AO information as instructed above.

# Other Designated Contacts

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

Delete this and all other instructions from your final version of this document.

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5‑1. Information System Management Point of Contact

| Information System Management Point of Contact | |
| --- | --- |
| Name | Iman Pemy |
| Title | Information System Management Point of Contact (POC) |
| Company / Organization | Pendeme Information Technology Group |
| Address | 11400 Westmoor Circle Suite 2501 Westminster CO 80021 US |
| Phone Number | 303-542-8492 |
| Email Address | Matthew.Holcomb@GDIT.com |

Table 5‑2. Information System Technical Point of Contact

| Information System Technical Point of Contact | |
| --- | --- |
| Name | Peter Harroun |
| Title | Information System Technical Point of Contact |
| Company / Organization | Pendeme Information Technology Group |
| Address | 11400 Westmoor Circle Suite 1014 Westminster Quebec 80021 Canada |
| Phone Number | 303-542-8492 |
| Email Address | Matthew.Holcomb@GDIT.com |

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

| Point of Contact | |
| --- | --- |
| Name | Peter Harroun |
| Title | General Point of Contact (POC) |
| Company / Organization | Pendeme Information Technology Group |
| Address | 11400 Westmoor Circle Suite 1014 Westminster Quebec 80021 Canada |
| Phone Number | 303-542-8492 |
| Email Address | Matthew.Holcomb@GDIT.com |

# Assignment of Security Responsibility

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6‑1. CSP Name Internal ISSO (or Equivalent) Point of Contact

| CSP Name Internal ISSO (or Equivalent) Point of Contact | |
| --- | --- |
| Name | Peter Harroun |
| Title | System Information System Security Officer (or Equivalent) |
| Company / Organization | Pendeme Information Technology Group |
| Address | 11400 Westmoor Circle Suite 1014 Westminster Quebec 80021 Canada |
| Phone Number | 303-542-8492 |
| Email Address | Matthew.Holcomb@GDIT.com |

Table 6‑2. AO Point of Contact

|  |  |
| --- | --- |
| AO Point of Contact | |
| Name | Malik Dechanel |
| Title | Authorizing Official |
| Organization | Volpe Information Technology Group |
| Address | 11400 2nd street NW Suite 114 Washington DC 20005 US |
| Phone Number | 301-542-8492 |
| Email Address | MDechanel@Fedramp.gov |

# Information System Operational Status

The system is currently in the life-cycle phase shown in Table 7‑1. System Status that follows. (Only operational systems can be granted an ATO).

Table 7‑1. System Status

| System Status | | |
| --- | --- | --- |
|  | Operational | The system is operating and in production. |
|  | Under Development | The system is being designed, developed, or implemented |
|  | Major Modification | The system is undergoing a major change, development, or transition. |
|  | Other | Explain: Click here to enter text. |

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

Delete this and all other instructions from your final version of this document.

# Information System Type

The GDIT Cloud makes use of unique managed service provider architecture layer(s).

## Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

|  |  |
| --- | --- |
| Question (Yes/No) | Conclusion |
| Does the system use virtual machines? | A no response means that system is most likely not a cloud. |
| Does the system have the ability to expand its capacity to meet customer demand? | A no response means that the system is most likely not a cloud. |
| Does the system allow the consumer to build anything other than servers? | A no response, means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS. |
| Does the system offer the ability to create databases? | A yes response means that the system is a PaaS. |
| Does the system offer various developer toolkits and APIs? | A yes response means that the system is a PaaS. |
| Does the system offer only applications that are available by obtaining a login? | A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS. |

The layers of the GDIT Cloud defined in this SSP are indicated in Table 8‑1. Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table 8‑1. Service Layers Represented in this SSP

| Service Provider Architecture Layers | | |
| --- | --- | --- |
|  | Software as a Service (SaaS) | Major Application |
|  | Platform as a Service (PaaS) | Major Application |
|  | Infrastructure as a Service (IaaS) | General Support System |
|  | Other | Explain: Click here to enter text. |

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

## Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the GDIT Cloud that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8‑2. Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table 8‑2. Cloud Deployment Model Represented in this SSP

| Service Provider Cloud Deployment Model | | |
| --- | --- | --- |
|  | Public | Cloud services and infrastructure supporting multiple organizations and agency clients |
|  | Private | Cloud services and infrastructure dedicated to a specific organization/agency and no other clients |
|  | Government Only Community | Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations |
|  | Hybrid | Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data)  Click here to enter text. |

## Leveraged Authorizations

Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher level layer represented by this SSP plans to leverage a lower layer’s Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write “None” in the first column of the table that follows. Add as many rows as necessary in the table that follows.

Delete this and all other instructions from your final version of this document.

The GDIT Cloud Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this GDIT Cloud are listed in Table 8‑3. Leveraged Authorizations that follows.

Table 8‑3. Leveraged Authorizations

| Leveraged Information System Name | Leveraged Service Provider Owner | Date Granted |
| --- | --- | --- |
| <Enter Leveraged information system name1> | <Enter service provider owner1> | <Date> |
| <Enter Leveraged information system name2> | <Enter service provider owner2> | <Date> |
| <Enter Leveraged information system name3> | <Enter service provider owner3> | <Date> |

# General System Description

This section includes a general description of the GDIT Cloud.

## System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system.

Delete this and all other instructions from your final version of this document.

## Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system’s Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].

**Additional FedRAMP Requirements and Guidance:**

**Guidance:** See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance

<https://www.fedramp.gov/documents/>

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9‑1. Authorization Boundary Diagram below.

|  |
| --- |
|  |

Figure 9‑1. Authorization Boundary Diagram

## Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9‑1. Personnel Roles and Privileges that follows.

Instruction: For an External User, write “Not Applicable” in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role type. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

Table 9‑1. Personnel Roles and Privileges

| Role | Internal or External | Privileged (P), Non-Privileged (NP), or No Logical Access (NLA) | Sensitivity Level | Authorized Privileges | Functions Performed |
| --- | --- | --- | --- | --- | --- |
| UNIX System Administrator | Internal | PP | Moderate | Full administrative access (root) | Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups |
| Client Administrator | External | NP | N/A | Portal administration | Add/remote client users. Create, modify and delete client applications |
| Program Director | Internal | NLA | Limited | N/A | Reviews, approves and enforces policy |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |
|  | Choose an item. | Choose an item. | Choose an item. |  |  |

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

## Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.

Delete this and all other instructions from your final version of this document.

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9‑2. Network Diagram mapping the data flow between components.

The following Figure 9‑2. Network Diagram(s) provides a visual depiction of the system network components that constitute GDIT Cloud.

|  |
| --- |
|  |

Figure 9‑2. Network Diagram

# System Environment And Inventory

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: Attachment 13, FedRAMP Inventory Workbook.

Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging or QA environments. Include the specific location of the alternate, backup and operational facilities.

In your description, also include a reference to Attachment 13, the system’s Integrated Inventory Workbook, which should provide a complete listing of the system’s components (operating systems/infrastructure, web applications/software, and databases). The Integrated Inventory Workbook should be maintained and updated monthly by the CSP, as part of continuous monitoring efforts. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook.

Delete this and all other instructions from your final version of this document.

## Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

The data flow in and out of the system boundaries is represented in Figure 10‑1. Data Flow Diagram below.

|  |
| --- |
|  |

Figure 10‑1. Data Flow Diagram

## Ports, Protocols and Services

The Table 10‑1. Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled “Used By” please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled “Purpose” indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.

Delete this and all other instructions from your final version of this document.

Table 10‑1. Ports, Protocols and Services

| Ports (TCP/UDP)\* | Protocols | Services | Purpose | Used By |
| --- | --- | --- | --- | --- |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |
| <Enter Port> | <Enter Protocols> | <Enter Services> | <Enter Purpose> | <Enter Used By> |

\* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

# System Interconnections

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13‑3 CA-3 Authorized Connections.

**Additional FedRAMP Requirements and Guidance:**

**Guidance**: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance

<https://www.fedramp.gov/documents/>

Delete this and all other instructions from your final version of this document.

Table 11‑1. System Interconnections below is consistent with Table 13‑3 CA-3 Authorized Connections.

Table 11‑1. System Interconnections

| SP\* IP Address and Interface | External Organization Name and IP Address of System | External Point of Contact and Phone Number | Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)\*\* | Data Direction  (incoming, outgoing, or both) | Information Being Transmitted | Port or Circuit Numbers |
| --- | --- | --- | --- | --- | --- | --- |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |
| <SP IP Address/Interface> | <External Org/IP> | <External Org POC>  <Phone 555-555-5555> | <Enter Connection Security> | Choose an item. | <Information Transmitted> | <Port/Circuit Numbers> |

\*Service Processor

\*\*Internet Protocol Security (IPSec), Virtual Private Network (VPN), Secure Sockets Layer (SSL)

# Laws, Regulations, Standards and Guidance

A summary of FedRAMP Laws and Regulations is included in Attachment 12, FedRAMP Laws and Regulations.

## Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on this web page: [Templates](https://www.fedramp.gov/templates).

Table 12‑1. GDIT Cloud IaaS Laws and Regulations includes additional laws and regulations specific to GDIT Cloud IaaS.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional laws and regulations that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table 12‑1. GDIT Cloud IaaS Laws and Regulations

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

## Applicable Standards and Guidance

The FedRAMP Standards and Guidance be found on this web page: [Templates](https://www.fedramp.gov/templates)

Table 12‑2. GDIT Cloud IaaS Standards and Guidance includes in this section any additional standards and guidance specific to GDIT Cloud IaaS.

Instruction: The information system name is a repeatable field that is populated when the Title Page is completed. If the CSP does not have additional standards or guidance that it must follow, please specify "N/A" in the table.

Delete this and all other instructions from your final version of this document.

Table 12‑2. GDIT Cloud IaaS Standards and Guidance

|  |  |  |  |
| --- | --- | --- | --- |
| Identification Number | Title | Date | Link |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |
| <Reference ID> | <Reference Title> | <Ref Date> | <Reference Link> |

# Minimum Security Controls

Security controls must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards apply. Some of the control baselines have enhanced controls which are indicated in parentheses.

Security controls that are representative of the sensitivity of GDIT Cloud are described in the sections that follow. Security controls that are designated as “Not Selected” or “Withdrawn by NIST” are not described unless they have additional FedRAMP controls. Guidance on how to describe the implemented standard can be found in NIST 800-53, Rev 4. Control enhancements are marked in parentheses in the sensitivity columns.

Systems that are categorized as FIPS 199 Low use the controls designated as Low, systems categorized as FIPS 199 Moderate use the controls designated as Moderate and systems categorized as FIPS 199 High use the controls designated as High. A summary of which security standards pertain to which sensitivity level is found in Table 13‑1. Summary of Required Security Controls that follows.

Table 13‑1. Summary of Required Security Controls

| ID | Control Description | Sensitivity Level | | |
| --- | --- | --- | --- | --- |
| Low | Moderate | High |
| AC | Access Control | | | |
| AC-1 | Access Control Policy and Procedures | AC-1 | AC-1 | AC-1 |
| AC-2 | Account Management | AC-2 | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (12) | AC-2 (1) (2) (3) (4) (5) (7) (9) (10) (11) (12) (13) |
| AC-3 | Access Enforcement | AC-3 | AC-3 | AC-3 |
| AC-4 | Information Flow Enforcement | Not Selected | AC-4 (21) | AC-4 (8) (21) |
| AC-5 | Separation of Duties | Not Selected | AC-5 | AC-5 |
| AC-6 | Least Privilege | Not Selected | AC-6 (1) (2) (5) (9) (10) | AC-6 (1) (2) (3) (5) (7) (8) (9) (10) |
| AC-7 | Unsuccessful Logon Attempts | AC-7 | AC-7 | AC-7 (2) |
| AC-8 | System Use Notification | AC-8 | AC-8 | AC-8 |
| AC-10 | Concurrent Session Control | Not Selected | AC-10 | AC-10 |
| AC-11 | Session Lock | Not Selected | AC-11 (1) | AC-11 (1) |
| AC-12 | Session Termination | Not Selected | AC-12 | AC-12 (1) |
| AC-14 | Permitted Actions Without Identification or Authentication | AC-14 | AC-14 | AC-14 |
| AC-17 | Remote Access | AC-17 | AC-17 (1) (2) (3) (4) (9) | AC-17 (1) (2) (3) (4) (9) |
| AC-18 | Wireless Access | AC-18 | AC-18 (1) | AC-18 (1) (3) (4) (5) |
| AC-19 | Access Control for Mobile Devices | AC-19 | AC-19 (5) | AC-19 (5) |
| AC-20 | Use of External Information Systems | AC-20 | AC-20 (1) (2) | AC-20 (1) (2) |
| AC-21 | Information Sharing | Not Selected | AC-21 | AC-21 |
| AC-22 | Publicly Accessible Content | AC-22 | AC-22 | AC-22 |
| AT | Awareness and Training | | | |
| AT-1 | Security Awareness and Training Policy and Procedures | AT-1 | AT-1 | AT-1 |
| AT-2 | Security Awareness Training | AT-2 | AT-2 (2) | AT-2 (2) |
| AT-3 | Role-Based Security Training | AT-3 | AT-3 | AT-3 (3) (4) |
| AT-4 | Security Training Records | AT-4 | AT-4 | AT-4 |
| AU | Audit and Accountability | | | |
| AU-1 | Audit and Accountability Policy and Procedures | AU-1 | AU-1 | AU-1 |
| AU-2 | Audit Events | AU-2 | AU-2 (3) | AU-2 (3) |
| AU-3 | Content of Audit Records | AU-3 | AU-3 (1) | AU-3 (1) (2) |
| AU-4 | Audit Storage Capacity | AU-4 | AU-4 | AU-4 |
| AU-5 | Response to Audit Processing Failures | AU-5 | AU-5 | AU-5 (1) (2) |
| AU-6 | Audit Review, Analysis and Reporting | AU-6 | AU-6 (1) (3) | AU-6 (1) (3) (4) (5) (6) (7) (10) |
| AU-7 | Audit Reduction and Report Generation | Not Selected | AU-7 (1) | AU-7 (1) |
| AU-8 | Time Stamps | AU-8 | AU-8 (1) | AU-8 (1) |
| AU-9 | Protection of Audit Information | AU-9 | AU-9 (2) (4) | AU-9 (2) (3) (4) |
| AU-10 | Non-repudiation | Not Selected | Not Selected | AU-10 |
| AU-11 | Audit Record Retention | AU-11 | AU-11 | AU-11 |
| AU-12 | Audit Generation | AU-12 | AU-12 | AU-12 (1) (3) |
| CA | Security Assessment and Authorization | | | |
| CA-1 | Security Assessment and Authorization Policies and Procedures | CA-1 | CA-1 | CA-1 |
| CA-2 | Security Assessments | CA-2 (1) | CA-2 (1) (2) (3) | CA-2 (1) (2) (3) |
| CA-3 | System Interconnections | CA-3 | CA-3 (3) (5) | CA-3 (3) (5) |
| CA-5 | Plan of Action and Milestones | CA-5 | CA-5 | CA-5 |
| CA-6 | Security Authorization | CA-6 | CA-6 | CA-6 |
| CA-7 | Continuous Monitoring | CA-7 | CA-7 (1) | CA-7 (1) (3) |
| CA-8 | Penetration Testing | Not Selected | CA-8 (1) | CA-8 (1) |
| CA-9 | Internal System Connections | CA-9 | CA-9 | CA-9 |
| CM | Configuration Management | | | |
| CM-1 | Configuration Management Policy and Procedures | CM-1 | CM-1 | CM-1 |
| CM-2 | Baseline Configuration | CM-2 | CM-2 (1) (2) (3) (7) | CM-2 (1) (2) (3) (7) |
| CM-3 | Configuration Change Control | Not Selected | CM-3 (2) | CM-3 (1) (2) (4) (6) |
| CM-4 | Security Impact Analysis | CM-4 | CM-4 | CM-4 (1) |
| CM-5 | Access Restrictions for Change | Not Selected | CM-5 (1) (3) (5) | CM-5 (1) (2) (3) (5) |
| CM-6 | Configuration Settings | CM-6 | CM-6 (1) | CM-6 (1) (2) |
| CM-7 | Least Functionality | CM-7 | CM-7 (1) (2) (5)\* | CM-7 (1) (2) (5) |
| CM-8 | Information System Component Inventory | CM-8 | CM-8 (1) (3) (5) | CM-8 (1) (2) (3) (4) (5) |
| CM-9 | Configuration Management Plan | Not Selected | CM-9 | CM-9 |
| CM-10 | Software Usage Restrictions | CM-10 | CM-10 (1) | CM-10 (1) |
| CM-11 | User-Installed Software | CM-11 | CM-11 | CM-11 (1) |
| \*FedRAMP does not include CM-7 (4) in the Moderate Baseline. NIST supplemental guidance states that CM-7 (4) is not required if (5) is implemented. | | | | |
| CP | Contingency Planning | | | |
| CP-1 | Contingency Planning Policy and Procedures | CP-1 | CP-1 | CP-1 |
| CP-2 | Contingency Plan | CP-2 | CP-2 (1) (2) (3) (8) | CP-2 (1) (2) (3) (4) (5) (8) |
| CP-3 | Contingency Training | CP-3 | CP-3 | CP-3 (1) |
| CP-4 | Contingency Plan Testing | CP-4 | CP-4 (1) | CP-4 (1) (2) |
| CP-6 | Alternate Storage Site | Not Selected | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Alternate Processing Site | Not Selected | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| CP-8 | Telecommunications Services | Not Selected | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | Information System Backup | CP-9 | CP-9 (1) (3) | CP-9 (1) (2) (3) (5) |
| CP-10 | Information System Recovery and Reconstitution | CP-10 | CP-10 (2) | CP-10 (2) (4) |
| IA | Identification and Authentication | | | |
| IA-1 | Identification and Authentication Policy and Procedures | IA-1 | IA-1 | IA-1 |
| IA-2 | Identification and Authentication (Organizational Users) | IA-2 (1) (12) | IA-2 (1) (2) (3) (5) (8) (11) (12) | IA-2 (1) (2) (3) (4) (5) (8) (9) (11) (12) |
| IA-3 | Device Identification and Authentication | Not Selected | IA-3 | IA-3 |
| IA-4 | Identifier Management | IA-4 | IA-4 (4) | IA-4 (4) |
| IA-5 | Authenticator Management | IA-5 (1) (11) | IA-5 (1) (2) (3) (4) (6) (7) (11) | IA-5 (1) (2) (3) (4) (6) (7) (8) (11) (13) |
| IA-6 | Authenticator Feedback | IA-6 | IA-6 | IA-6 |
| IA-7 | Cryptographic Module Authentication | IA-7 | IA-7 | IA-7 |
| IA-8 | Identification and Authentication (Non-Organizational Users) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) | IA-8 (1) (2) (3) (4) |
| IR | Incident Response | | | |
| IR-1 | Incident Response Policy and Procedures | IR-1 | IR-1 | IR-1 |
| IR-2 | Incident Response Training | IR-2 | IR-2 | IR-2 (1) (2) |
| IR-3 | Incident Response Testing | Not Selected | IR-3 (2) | IR-3 (2) |
| IR-4 | Incident Handling | IR-4 | IR-4 (1) | IR-4 (1) (2) (3) (4) (6) (8) |
| IR-5 | Incident Monitoring | IR-5 | IR-5 | IR-5 (1) |
| IR-6 | Incident Reporting | IR-6 | IR-6 (1) | IR-6 (1) |
| IR-7 | Incident Response Assistance | IR-7 | IR-7 (1) (2) | IR-7 (1) (2) |
| IR-8 | Incident Response Plan | IR-8 | IR-8 | IR-8 |
| IR-9 | Information Spillage Response | Not Selected | IR-9 (1) (2) (3) (4) | IR-9 (1) (2) (3) (4) |
| MA | Maintenance | | | |
| MA-1 | System Maintenance Policy and Procedures | MA-1 | MA-1 | MA-1 |
| MA-2 | Controlled Maintenance | MA-2 | MA-2 | MA-2 (2) |
| MA-3 | Maintenance Tools | Not Selected | MA-3 (1) (2) (3) | MA-3 (1) (2) (3) |
| MA-4 | Nonlocal Maintenance | MA-4 | MA-4 (2) | MA-4 (2) (3) (6) |
| MA-5 | Maintenance Personnel | MA-5 | MA-5 (1) | MA-5 (1) |
| MA-6 | Timely Maintenance | Not Selected | MA-6 | MA-6 |
| MP | Media Protection | | | |
| MP-1 | Media Protection Policy and Procedures | MP-1 | MP-1 | MP-1 |
| MP-2 | Media Access | MP-2 | MP-2 | MP-2 |
| MP-3 | Media Marking | Not Selected | MP-3 | MP-3 |
| MP-4 | Media Storage | Not Selected | MP-4 | MP-4 |
| MP-5 | Media Transport | Not Selected | MP-5 (4) | MP-5 (4) |
| MP-6 | Media Sanitization | MP-6 | MP-6 (2) | MP-6 (1) (2) (3) |
| MP-7 | Media Use | MP-7 | MP-7 (1) | MP-7 (1) |
| PE | Physical and Environmental Protection | | | |
| PE-1 | Physical and Environmental Protection Policy and Procedures | PE-1 | PE-1 | PE-1 |
| PE-2 | Physical Access Authorizations | PE-2 | PE-2 | PE-2 |
| PE-3 | Physical Access Control | PE-3 | PE-3 | PE-3 (1) |
| PE-4 | Access Control for Transmission Medium | Not Selected | PE-4 | PE-4 |
| PE-5 | Access Control for Output Devices | Not Selected | PE-5 | PE-5 |
| PE-6 | Monitoring Physical Access | PE-6 | PE-6 (1) | PE-6 (1) (4) |
| PE-8 | Visitor Access Records | PE-8 | PE-8 | PE-8 (1) |
| PE-9 | Power Equipment and Cabling | Not Selected | PE-9 | PE-9 |
| PE-10 | Emergency Shutoff | Not Selected | PE-10 | PE-10 |
| PE-11 | Emergency Power | Not Selected | PE-11 | PE-11 (1) |
| PE-12 | Emergency Lighting | PE-12 | PE-12 | PE-12 |
| PE-13 | Fire Protection | PE-13 | PE-13 (2) (3) | PE-13 (1) (2) (3) |
| PE-14 | Temperature and Humidity Controls | PE-14 | PE-14 (2) | PE-14 (2) |
| PE-15 | Water Damage Protection | PE-15 | PE-15 | PE-15 (1) |
| PE-16 | Delivery and Removal | PE-16 | PE-16 | PE-16 |
| PE-17 | Alternate Work Site | Not Selected | PE-17 | PE-17 |
| PE-18 | Location of Information System Components | Not Selected | Not Selected | PE-18 |
| PL | Planning | | | |
| PL-1 | Security Planning Policy and Procedures | PL-1 | PL-1 | PL-1 |
| PL-2 | System Security Plan | PL-2 | PL-2 (3) | PL-2 (3) |
| PL-4 | Rules of Behavior | PL-4 | PL-4 (1) | PL-4 (1) |
| PL-8 | Information Security Architecture | Not Selected | PL-8 | PL-8 |
| PS | Personnel Security | | | |
| PS-1 | Personnel Security Policy and Procedures | PS-1 | PS-1 | PS-1 |
| PS-2 | Position Risk Designation | PS-2 | PS-2 | PS-2 |
| PS-3 | Personnel Screening | PS-3 | PS-3 (3) | PS-3 (3) |
| PS-4 | Personnel Termination | PS-4 | PS-4 | PS-4 (2) |
| PS-5 | Personnel Transfer | PS-5 | PS-5 | PS-5 |
| PS-6 | Access Agreements | PS-6 | PS-6 | PS-6 |
| PS-7 | Third-Party Personnel Security | PS-7 | PS-7 | PS-7 |
| PS-8 | Personnel Sanctions | PS-8 | PS-8 | PS-8 |
| RA | Risk Assessment | | | |
| RA-1 | Risk Assessment Policy and Procedures | RA-1 | RA-1 | RA-1 |
| RA-2 | Security Categorization | RA-2 | RA-2 | RA-2 |
| RA-3 | Risk Assessment | RA-3 | RA-3 | RA-3 |
| RA-5 | Vulnerability Scanning | RA-5 | RA-5 (1) (2) (3) (5) (6) (8) | RA-5 (1) (2) (3) (4) (5) (6) (8) (10) |
| SA | System and Services Acquisition | | | |
| SA-1 | System and Services Acquisition Policy and Procedures | SA-1 | SA-1 | SA-1 |
| SA-2 | Allocation of Resources | SA-2 | SA-2 | SA-2 |
| SA-3 | System Development Life Cycle | SA-3 | SA-3 | SA-3 |
| SA-4 | Acquisition Process | SA-4 (10) | SA-4 (1) (2) (8) (9) (10) | SA-4 (1) (2) (8) (9) (10) |
| SA-5 | Information System Documentation | SA-5 | SA-5 | SA-5 |
| SA-8 | Security Engineering Principles | Not Selected | SA-8 | SA-8 |
| SA-9 | External Information System Services | SA-9 | SA-9 (1) (2) (4) (5) | SA-9 (1) (2) (4) (5) |
| SA-10 | Developer Configuration Management | Not Selected | SA-10 (1) | SA-10 (1) |
| SA-11 | Developer Security Testing and Evaluation | Not Selected | SA-11 (1) (2) (8) | SA-11 (1) (2) (8) |
| SA-12 | Supply Chain Protection | Not Selected | Not Selected | SA-12 |
| SA-15 | Development Process, Standards and Tools | Not Selected | Not Selected | SA-15 |
| SA-16 | Developer-Provided Training | Not Selected | Not Selected | SA-16 |
| SA-17 | Developer Security Architecture and Design | Not Selected | Not Selected | SA-17 |
| SC | System and Communications Protection | | | |
| SC-1 | System and Communications Protection Policy and Procedures | SC-1 | SC-1 | SC-1 |
| SC-2 | Application Partitioning | Not Selected | SC-2 | SC-2 |
| SC-3 | Security Function Isolation | Not Selected | Not Selected | SC-3 |
| SC-4 | Information in Shared Resources | Not Selected | SC-4 | SC-4 |
| SC-5 | Denial of Service Protection | SC-5 | SC-5 | SC-5 |
| SC-6 | Resource Availability | Not Selected | SC-6 | SC-6 |
| SC-7 | Boundary Protection | SC-7 | SC-7 (3) (4) (5) (7) (8) (12) (13) (18) | SC-7 (3) (4) (5) (7) (8) (10) (12) (13) (18) (20) (21) |
| SC-8 | Transmission Confidentiality and Integrity | Not Selected | SC-8 (1) | SC-8 (1) |
| SC-10 | Network Disconnect | Not Selected | SC-10 | SC-10 |
| SC-12 | Cryptographic Key Establishment and Management | SC-12 | SC-12 (2) (3) | SC-12 (1) (2) (3) |
| SC-13 | Cryptographic Protection | SC-13 | SC-13 | SC-13 |
| SC-15 | Collaborative Computing Devices | SC-15 | SC-15 | SC-15 |
| SC-17 | Public Key Infrastructure Certificates | Not Selected | SC-17 | SC-17 |
| SC-18 | Mobile Code | Not Selected | SC-18 | SC-18 |
| SC-19 | Voice Over Internet Protocol | Not Selected | SC-19 | SC-19 |
| SC-20 | Secure Name / Address Resolution Service (Authoritative Source) | SC-20 | SC-20 | SC-20 |
| SC-21 | Secure Name / Address Resolution Service (Recursive or Caching Resolver) | SC-21 | SC-21 | SC-21 |
| SC-22 | Architecture and Provisioning for Name / Address Resolution Service | SC-22 | SC-22 | SC-22 |
| SC-23 | Session Authenticity | Not Selected | SC-23 | SC-23 (1) |
| SC-24 | Fail in Known State | Not Selected | Not Selected | SC-24 |
| SC-28 | Protection of Information at Rest | Not Selected | SC-28 (1) | SC-28 (1) |
| SC-39 | Process Isolation | SC-39 | SC-39 | SC-39 |
| SI | System and Information Integrity | | | |
| SI-1 | System and Information Integrity Policy and Procedures | SI-1 | SI-1 | SI-1 |
| SI-2 | Flaw Remediation | SI-2 | SI-2 (2) (3) | SI-2 (1) (2) (3) |
| SI-3 | Malicious Code Protection | SI-3 | SI-3 (1) (2) (7) | SI-3 (1) (2) (7) |
| SI-4 | Information System Monitoring | SI-4 | SI-4 (1) (2) (4) (5) (14) (16) (23) | SI-4 (1) (2) (4) (5) (11) (14) (16) (18) (19) (20) (22) (23) (24) |
| SI-5 | Security Alerts, Advisories and Directives | SI-5 | SI-5 | SI-5 (1) |
| SI-6 | Security Function Verification | Not Selected | SI-6 | SI-6 |
| SI-7 | Software, Firmware and Information Integrity | Not Selected | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (14) |
| SI-8 | Spam Protection | Not Selected | SI-8 (1) (2) | SI-8 (1) (2) |
| SI-10 | Information Input Validation | Not Selected | SI-10 | SI-10 |
| SI-11 | Error Handling | Not Selected | SI-11 | SI-11 |
| SI-12 | Information Handling and Retention | SI-12 | SI-12 | SI-12 |
| SI-16 | Memory Protection | SI-16 | SI-16 | SI-16 |

Note: The -1 Controls (AC-1, AU-1, SC-1, etc.) cannot be inherited and must be provided in some way by the service provider.

Instruction: In the sections that follow, describe the information security control as it is implemented on the system. All controls originate from a system or from a business process. It is important to describe where the control originates from so that it is clear whose responsibility it is to implement, manage and monitor the control. In some cases, the responsibility is shared by a CSP and by the customer. Use the definitions in the table that follows to indicate where each security control originates from.

Throughout this SSP, policies and procedures must be explicitly referenced (title and date or version) so that it is clear which document is being referred to. Section numbers or similar mechanisms should allow the reviewer to easily find the reference.

For SaaS and PaaS systems that are inheriting controls from an IaaS (or anything lower in the stack), the “inherited” check box must be checked and the implementation description must simply say “inherited.” FedRAMP reviewers will determine whether the control-set is appropriate or not.

In Section 13, the NIST term "organization defined" must be interpreted as being the CSP's responsibility unless otherwise indicated. In some cases, the JAB has chosen to define or provide parameters, in others they have left the decision up to the CSP.

Please note: CSPs should not modify the control requirement text, including the parameter assignment instructions and additional FedRAMP requirements. CSP responses must be documented in the “Control Summary Information” and “What is the solution and how is it implemented?” tables.

Delete this and all other instructions from your final version of this document.

The definitions in Table 13‑2. Control Origination and Definitions indicate where each security control originates.

Table 13‑2. Control Origination and Definitions

| Control Origination | Definition | Example |
| --- | --- | --- |
| Service Provider Corporate | A control that originates from the PITG 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 PITG and the control is not part of the standard 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 PITG. | There are 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 PITG and partially by the customer. | Security awareness training must be conducted by both the CSPN and the customer. |
| Inherited from pre-existing FedRAMP Authorization | A control that is inherited from another PITG system that has already received a FedRAMP Authorization. | A PaaS or SaaS provider inherits PE controls from an IaaS provider. |

\*Hyper Text Transport Protocol (http)

Responsible Role indicates the role of CSP employee who can best respond to questions about the particular control that is described.

## Access Control (AC)

### AC-1 Access Control Policy and Procedures Requirements (L) (M)

The organization:

1. Develops, documents and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the access control policy and associated access controls; and
2. Reviews and updates the current:
   1. Access control policy [FedRAMP Assignment: at least every 3 years]; and
   2. Access control procedures [FedRAMP Assignment: at least annually].

| AC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AC-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter AC-1(b)(1): at least every 3 years | |
| Parameter AC-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.1. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, access control policy and associated access controls in the GDIT Cloud’s GDIT-OC-PRO-AC Access Controls Procedures. These policies are stored in the GDIT Cloud's secure SharePoint site. |
| Part b1 | The ISSO reviews and updates the policy at least every three years and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associated Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |
| Part b2 | Click or tap here to enter text. |

### AC-2 Account Management (L) (M)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
5. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
7. Monitors the use of information system accounts;
8. Notifies account managers:
   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;
9. Authorizes access to the information system based on:
   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;
10. Reviews accounts for compliance with account management requirements [FedRAMP Assignment: at least annually]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AC-2(a): Organization-defined information system account types:; Individual; Group; Service; Guest Anonymous; Temporary; Administrator | |
| Parameter AC-2(e): ISSO and Cloud System Manager | |
| Parameter AC-2(f): organization-defined procedures or conditions | |
| Parameter AC-2(j): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | . |
| Part b |  |
| Part c |  |
| Part d | . |
| Part e | . |
| Part f | Once the GDIT Cloud System Manager approves all system individual accounts to be created or changed through the Cherwell ticket, then the System Administrator creates, enables, modifies, disables, and removes GDIT Cloud system accounts in accordance with system account policies and procedures defined in the GDIT Cloud Access Management Process and Procedures Guide, 0.8. This includes all account types and categories, as listed in Part a: Non-privileged Privileged Domain Admin (DA) All system account activities are authorized through the Cherwell ticketing system. Account Creation, Enablement, and Modification System account modification requires approval from the GDIT Cloud ISSO prior to performing account modification. The exception to this is downgrading an account from privileged to non-privileged access; that is, based on a role change the account system administrator can downgrade a user’s access prior to notifying the ISSO of such a change. Account Disablement and Removal System account disablement can be accomplished prior to notifying the GDIT Cloud ISSO. However, the ISSO is notified as soon as possible when an account is disabled, along with the reason for disabling the account. Account removal requires GDIT Cloud ISSO approval. Account disablement is tracked as a ticket in Cherwell and pertains to the following systems: Cherwell Traverse Active Directory AlienVault RSA Nessus Security Center vCenter TACACS Password Manager Pro Cisco Security Operations Manager Customer Responsibility The Customer system administrator is responsible for creating, enabling, modifying, disabling, and removing users’ accounts within the Customer environment. |
| Part g | Security Analysts monitor the use of all GDIT Cloud system accounts (with no exception) through alerts generated by Alien Vault. System Administrators configure the GDIT Cloud MMS SIEM to send alerts for system configuration changes and user account creations, enablement, deletions, modifications, and removal. The alerts appear on the Alien Vault user interface as well as generating an ‘event’ in the Cherwell ticketing system. The Security Analysts monitor the event queue 24x7 for any new events. They can either be dismissed as false positive/authorized/allowed or provoke the analyst to generate an incident ticket. The incident ticket process is consistent with processes described in the IR family of controls, specifically IR-4 Incident Handling within this document. Both the alert in AlienVault and the event in Cherwell are independently analyzed. System and account monitoring is also described in SI-4. |
| Part h | As defined in the GDIT Cloud Employee On-Boarding and Off-Boarding , GDIT Human Resources department (HR) notifies account managers when: Accounts are no longer required Users are terminated or transferred Account Managers have responsibility for understanding changes to system usage or need-to-know for the users for which they are responsible. The notification is performed in the GDIT email system and sent to a distribution list. Customer Responsibility The Customer is responsible for notifying Cloud personnel when Customer accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes. |
| Part i | The GDIT Cloud System Manager and ISSO authorize access to the information system based on: A valid access authorization Intended system usage based on missions/business functions All personnel requiring access to the information system are granted access only after there is a documented access request submitted to the GDIT Cloud ticketing system and approved by the System Manager and GDIT Cloud ISSO. The access request includes the intended use, purpose, and reason for system use for granting access to the information system. The GDIT Cloud Employee On-Boarding and Off-Boarding establishes a formal access process to justify, authorize, and document the need for access to the information system: Confirmation of new hire. Submit request for accounts to General Dynamics IT (GDIT). Notify Operations and Engineering Managers about the new hire. Notify Facility Security Officer (FSO) about the new hire: Badging Facility access (the access level is determined by the manager) New hire orientation. If applicable: For non-GDIT employees a signed GDIT Non-Disclosure Agreement (NDA) is required. Submit request for GDIT Cloud accounts (varies per role). GDIT Cloud accounts created. |
| Part j | The GDIT Cloud ISSO reviews all system accounts and individual assigned role(s) that contains the access privileges (specified in Attachment 10: Roles and Privileges Matrix) for compliance with account management requirements annually as part of the continuous monitoring process and to ensure all system accounts associated with terminated, transferred or downgraded personnel have been properly removed or maintained. In response to the ticket, the system administrator generates a report of the accounts assigned to each group (role). The ISSO and management team evaluate the report to review that each assigned account is assigned the appropriate role(s). Tasks are generated from the Cherwell ticket to make any required updates. The NOC or Directory Services will then make those updates, depending on the authorization required for each group. The GDIT Cloud Security Calendar, maintained on the secure GDIT Cloud SharePoint site, initiates the annual System Accounts Review. The results of the review are recorded in the Cherwell ticket. In response to the ticket, the system administrator generates a report of the accounts assigned to each group (role). The ISSO and management team evaluate the report to review that each assigned account is assigned the appropriate role(s). Tasks are generated from the Cherwell ticket to make any required updates. The NOC or Directory Services will then make those updates, depending on the authorization required for each group. Customer Responsibility The Customer is responsible for reviewing all system accounts for compliance with account management requirements annually as part of their continuous monitoring process and to ensure accounts associated with terminated, transferred or downgraded personnel are properly removed or maintained. |
| Part k | This part is NA. According to GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.1, no Group or Shared accounts are allowed within the GDIT Cloud environment, i.e., no instance of a single group account with a shared password. Customer Responsibility Customers are responsible for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. |

### AC-3 Access Enforcement (L) (M) (H)

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

| AC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| AC-3 What is the solution and how is it implemented? |
| --- |
| The access control process as defined in the GDIT Cloud Access Management Process and Procedures Guide, enforces approved authorizations for logical access to information and system resources in accordance with KA 10558, How To: GDIT Cloud Account Creation, maintained in Cherwell. The Account Manager bases authorizations on user, role, and business need as required to perform essential tasks associated with an individual’s login credentials. In addition to user accounts, MS Active Directory is the authentication mechanism for most of the components of the GDIT Cloud, including the Firewalls, Cloud Compute, and Cloud storage. The policies configured in the MS Active Directory for account expiration, lockout, and other parameters apply to all user accounts and components uniformly. Customer Responsibility The Customer is responsible for enforcing approved authorizations for logical access to information and system resources in accordance with its applicable access control policies in the Customer environment. |

### AC-7 Unsuccessful Login Attempts (L) (M)

The organization:

1. Enforces a limit of [FedRAMP Assignment: not more than three (3)] consecutive invalid logon attempts by a user during a [FedRAMP Assignment: fifteen (15) minutes]; and
2. Automatically [Selection: locks the account/node for a [FedRAMP Assignment: thirty (30) minutes]; delays next logon prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded.

| AC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter AC-7(a)-1: not more than three | |
| Parameter AC-7(a)-2: fifteen minutes | |
| Parameter AC-7(b)-1: locks the account/node for thirty minutes | |
| Parameter AC-7(b)-2: (b )-2 organization-defined delay algorithm | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud enforces a limit of not more than three consecutive invalid logon attempts by a user during a fifteen minute timeframe, as follows: The System Administrator establishes login settings in the Active Directory GPO to enforcea limit ofthree (3) consecutive invalidlogin attempts during a 15 minute period before lockingtheaccount. When the threshold for unsuccessful logins is reached, Active Directory locks the account. When the account is locked out Active Directory, subsequent attempts to log in to devices fail because the account and its security group membership will not be obtainable due to it being locked out. This setting applies to the accounts that are used to log in to the Business Portal as well The AD GPO login enforcement also protects all components in the GDIT Cloud because they all point to AD, as follows: NetworkACSRSA Authentication AD (authorization) RSA-enable-devices AD (authorization) Non-RSA devices, then JumpServer RSAAD (authorization) When logging into a network device, credentials are sent to the ACS server.  These credentials are passed off to the RSA server for authentication.  Once validated, the account is checked against Active Directory for Security Group membership.  If the account is in the proper security group in Active Directory the user is granted access to the device with the level of permission specified in ACS for that security group. |
| Part b | The GDIT Cloud information system automatically locksthe account/node whenthemaximumnumberofunsuccessfullogin attemptsis exceeded. This applies to all Active Directory accounts and GDIT Cloud components, as well as the Portal. In order to unlock an account, the user must call the GDIT Cloud Service Desk (available 24/7) and request that the account be unlocked. |

### AC-8 System Use Notification (L) (M) (H)

The information system:

1. Displays to users [Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:
   1. Users are accessing a U.S. Government information system;
   2. Information system usage may be monitored, recorded, and subject to audit;
   3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
   4. Use of the information system indicates consent to monitoring and recording;
2. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and
3. For publicly accessible systems:
   1. Displays system use information [Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)], before granting further access;
   2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
   3. Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter AC-8(a): organization-defined system use notification message or banner | |
| Parameter AC-8(c)-1: ; Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB.; Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB.; Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.; Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud ISSO and the GDIT Cloud System Administrators ensurethat the GDIT Cloud system displays an approved “system use”notification messagebefore granting system access to users. Themessageinforms the GDIT Cloud internal user: That theuseris accessing a GDIT information system That system usagemay bemonitored, recorded, and subject to audit That unauthorized useofthe system is prohibited and subject to criminal and civil penalties That theuseofthe system indicates consent to monitoring and recording \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* This is a U.S. Federal Government computer system that is "FOR OFFICIAL USE ONLY." This information form this system is subject to be monitored, recorded and/or audited. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* This is a U.S. Federal Government computer system that is "FOR OFFICIAL USE ONLY." This information form this system is subject to be monitored, recorded and/or audited. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* |
| Part b | TheGDIT Cloud system usenotification message remains on thescreen until theusertakes explicit actions by clicking on a button that signifies agreeing to the terms of use. |
| Part c | All GDIT Cloud publically-accessible portals display a warning banner before users are granted access to the GDIT Cloud. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* This is a U.S. Federal Government computer system that is "FOR OFFICIAL USE ONLY." This information system is subject to be monitored, recorded and/or audited. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* This is a U.S. Federal Government computer system that is "FOR OFFICIAL USE ONLY." This information system is subject to be monitored, recorded and/or audited. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution. \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* WARNING\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Customer users access two systems within the IaaS that require agreeing to a system use notification message before being allowed access: Cherwell VPN |

Additional FedRAMP Requirements and Guidance

Requirement 1: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement 2: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO. If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement 3: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

| AC-8 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Req. 1 When GDIT Cloud personnel log onto the GDIT Cloud system, they are reminded of the system use requirements for GDIT Cloud system access bya system use notification banner. The elements of the cloud environment that require a system use notification banner are as follows: All Microsoft and Linux systems All external access to the GDIT Cloud (Remote access and Portals). This is provided to the JAB for approval and acceptance. Customer Responsibility The customer is responsible for ensuring that a system usenotification warning banner displays on all systems within the Customer environment. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| AC-8 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Req. 2 Tripwire performs automated configuration baseline checks on the system use warning banners for Microsoft and Linux systems. All other systems (Remote access and all Portals) are verified manually by the ISSO. The ISSO performs a verification of the system use notification message annually. The verification is governed by the continuous monitoring process and initiated by the GDIT Cloud Security Calendar that is maintained on the GDIT Cloud SharePoint site. The results of the review are recorded in the Cherwell ticket. This is provided to the JAB for approval and acceptance. Customer Responsibility The customer is responsible for ensuring that a system usenotification warning banner is verified on all of their systems within their environments. |
| Req. 2 | Req. 3 The automated configuration baseline check is described in Req. 2. For those systems that do not use Tripwire for configuration baseline verification (remote access and all Portals), the ISSO performs a verification of notification message annually. The verification is governed by the continuous monitoring process and initiated by the GDIT Cloud Security Calendar that is maintained on the GDIT Cloud SharePoint site. The results of the review are recorded in the Cherwell ticket. This method of providing manual verification results is provided to the JAB for approval and acceptance. Customer Responsibility The customer is responsible for ensuring that a system usenotification warning banner is verified manually if an automated configuration baseline check cannot be performed on all of the systems within the customer environment. |
| Req. 3 | Click or tap here to enter text. |

### AC-14 Permitted Actions without Identification or Authentication (L) (M) (H)

The organization:

1. Identifies [Assignment: organization-defined user actions] that can be performed on the information system without identification or authentication consistent with organizational missions/business functions; and
2. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification or authentication.

| AC-14 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-14(a): No user actions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager does not authorize or approve any user actions to be performedon the GDIT Cloud information system without identification and authentication consistent with organizational missions/business functions as governed by SOP: GDIT Cloud Employee On-Boarding and Off-Boarding. |
| Part b | The GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.1 prohibits user actions in the GDIT Cloud environment without identification and authentication. Therefore, there is no supporting rationale in the security plan for user actions not requiring identification or authentication. |

### AC-17 Remote Access (L) (M) (H)

The organization:

1. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
2. Authorizes remote access to the information system prior to allowing such connections.

| AC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| AC-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Network Engineers establish and document remote access usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed, as follows: VPN Remote Access Usage restrictions: Available 24/7 to support operations and maintenance/monitoring Implementation Guidance: FIPS 140-2 encryption and 2- factor authentication on the VPN Website Remote Access Usage restrictions: Available 24/7 to support operations and implementation Implementation Guidance: HTTPS and FIPS 140-2 encryption and 2- factor authentication |
| Part b | The GDIT Cloud Account Managers authorize,monitor, and control allmethodsof remote accesstotheinformation systemincluding remote access forprivileged functions. The security group membership in AD serves as the control for logical access authorization enforcement. Authorizations are based on user, role, and need as required to perform essential tasks associated with an individual’s login credentials. MS Active Directory is the authentication mechanism for most of the components of the Information System, (including the Firewalls, Cloud Compute, and Cloud storage.) The policies configured in the MS Active Directory for account expiration, lockout, and other parameters apply to all aspects of the Information System uniformly. For access to the GDIT Cloud information system, all users are required to provide basic information (i.e. job category, nationality, program supported) prior to being granted access. This information is used as the foundation to allow or assign network access and to determine what network resources an individual may have. The GDIT Cloud information system enforces assigned authorizations in accordance with GDIT Cloud Policy related to System Access Control. The following implementation details correspond to all GDIT Cloud devices. Attributes taken into account in the logical authentication process are as follows: User ID + Password PIN + Token Host being accessed as identified by its IP address Host where access is being attempted from MS Active Directory System administrator creates user accounts within the MS Active Directory, and assigns the user ID to the appropriate MS Groups, to ensure that the User has the access commensurate with his or her role. The authorization enforcement mechanism for user accounts on the systems in the GDIT Cloud Information System is MS Active Directory. A role is implemented by creating a user group and granting that group permission to access certain hosts, identified as GDIT Cloud systems. Users can then be added to the appropriate group(s) to provide the appropriate access permissions. When a user attempts to access a system protected using MS Active Directory, the system not only passes the user credential, but also passes the hostname as well. If all of those items do not match the user permissions then the authentication request is denied. |

### AC-18 Wireless Access Restrictions (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and
2. Authorizes wireless access to the information system prior to allowing such connections.

| AC-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This control is N/A. The GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.1 prohibits wireless access to the GDIT Cloud. |
| Part b | This control is N/A. The GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.1 prohibits wireless access to the GDIT Cloud. |

### AC-19 Access Control for Portable and Mobile Systems (L) (M) (H)

The organization:

1. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices; and
2. Authorizes the connection of mobile devices to organizational information systems.

| AC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager has established the GDIT Cloud Rules of Behavior, as the policy governance of theissuance andusageof GDIT owned and controlledportable andmobiledevicesthat are the following: GDIT Cloud Laptops GDIT Cloud Iron Key and Aegis Padlock DT portable mobile media The GDIT Cloud adheres to the GDIT policy, SEC-POL-IT-21, Remote Access, Mobile Computing, and Telecommuting that identifies the appropriate usage of company issued portable devices such as Laptops and Mobile communication devices. |
| Part b | The System Manager has authorized connection authorization for the two permitted mobile devices in the GDIT Cloud are as follows: Laptops are an essential part of the mission for monitoring and managing the GDIT Cloud. Laptops can be connected to the network at any time and are authorized to be disconnected from the network and taken home for remote access in cases where the need arises because of problems or an incident. Usage restriction is covered by the GDIT Cloud Rules of Behavior . The System Manager authorizes use of the Iron Key and Aegis Padlock DT mobile devices in support of on-boarding (provisioning) of new customers. The Iron Key and Aegis Padlock DT mobile devices are used to transfer virtual systems from one location to another and to support movement of data required by customers. Usage restriction is covered by the GDIT Cloud Rules of Behavior . |

### AC-20 Use of External Information Systems (L) (M) (H)

The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

1. Access the information system from external information systems; and
2. Process, store, or transmit organization-controlled information using external information systems.

| AC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager prevents any external information systems being utilized to manage the GDIT Cloud environment. To achieve this, GDIT distributes to GDIT Cloud personnel approved GDIT Cloud laptops that are configured to support FIPS 140-2 encryption for exclusive use. Customer Responsibility Customer agencies are responsible for establishing and managing terms and conditions for the use of external systems within their environment. |
| Part b | According to the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.1, the GDIT Cloud does not permit the processing, storage, and/or transmission of GDIT Cloud information system-controlled information using external information systems. Customer Responsibility Customer agencies are responsible for defining, managing, processing, storing, and/or transmitting information that uses an external information system as part of their environment. |

### AC-22 Publicly Accessible Content (L) (M) (H)

The organization:

1. Designates individuals authorized to post information onto a publicly accessible information system;
2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
3. Reviews the proposed content of information prior to posting onto the publicly accessible information system to ensure that nonpublic information is not included; and
4. Reviews the content on the publicly accessible information system for nonpublic information [FedRAMP Assignment: at least quarterly] and removes such information, if discovered.

| AC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-22: Quarterly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AC-22 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This control is NA. The System Manager does not authorize individuals to post information onto a publicly accessible information system. Only Cloud subscribers may access the GDIT Cloud. |
| Part b | This control is NA. The System Manager does not authorize individuals to post information onto a publicly accessible information system. Only Cloud subscribers may access the GDIT Cloud. |
| Part c | This control is NA. The System Manager does not authorize individuals to post information onto a publicly accessible information system. Only Cloud subscribers may access the GDIT Cloud. |
| Part d | This control is NA. The System Manager does not authorize individuals to post information onto a publicly accessible information system. Only Cloud subscribers may access the GDIT Cloud. |

## Awareness and Training (AT)

### AT-1 Security Awareness and Training Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and
2. Reviews and updates the current:
   1. Security awareness and training policy [FedRAMP Assignment: at least every 3 years]; and
   2. Security awareness and training procedures [FedRAMP Assignment: at least annually].

| AT-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AT-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter AT-1(b)(1): at least every 3 years | |
| Parameter AT-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AT-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.2. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, security awareness and training controls in the GDIT Cloud’s GDIT-OC-PRO-AT Security Awareness and Training Procedures. All procedures are stored in an access controlled GDIT Cloud SharePoint site where version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### AT-2 Security Awareness (L) (M) (H)

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):

1. As part of initial training for new users;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AT-2(c): Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Training Department provides basic security awareness training to the system users (including managers, senior executives, and contractors), as part of initial training for new users. All staff receives initial security awareness training upon hire or when joining the GDIT Cloud team, according to the GDIT Cloud Employee On-Boarding and Off-Boarding. GDIT has implemented several policies and associated procedures to disseminate and review personnel security. These include the following: HR-MISC-404A New Employee Required Training– explicitly identifying required training for all new employees to complete within first 30 days of employment including Information Security Awareness (ISA) and Privacy and Security of Personal Information. SEC-POL-IT-34 Security Awareness and Training – explicitly identifying GDIT roles and responsibilities for implementing the security policy and explicitly requiring annual Information Security Awareness training for employees and other personnel with access to the GDIT network. As required by contract, GDIT Cloud personnel may receive customer security awareness training as stated in the contract and per customer security policies. Each time security awareness training is conducted, the employee signs an affirmation of compliance to the security policies. GDIT employees and contractors access GDIT corporate security awareness training through the GDIT learning management system (myLMS). All employees must complete the training when first hired and then again on an annual basis, regardless of which program the employee supports. Employees complete the following training sessions in myLMS: Annual Security Briefing Covers higher level security concepts including the following: Compliance and policy reminders Physical security (badges) Protection and handling of PII Identifying, handling, and protecting classified materials Guidelines for international travel Handling Non-US and foreign visitors Counterintelligence OPSEC and Social Networking Sites Security violations and reporting requirements Information Security Awareness Covers topics specific to the protection of information and information assets Passwords: Protecting Your Information Social Engineering: Manipulation in the Modern World Data Management Company Sensitive Information Culture of Responsibility (CoR) Training Overview of the HCSD Culture of Responsibility (CoR) policies and employee responsibilities related to the protection of customer constituent personal information. Note: GDIT may modify the contents to emphasize emerging threats. |
| Part b | The GDIT Training Department provides basic security awareness training to information system users (including managers, senior executives, and contractors), when required by information system changes. Any change to the GDIT Cloud must be approved by the CAB as described in the GDIT Cloud Change Management Process and Procedures Guide. The ISSO conducts a security impact assessment for every change request that includes the potential changes to the basic security awareness training as a result of change to the GDIT Cloud system. The type of basic security awareness training given based on information system changes would be solely dependent upon the type of change made. Given that this control covers basic level training, an example of a system change would be a change in how GDIT corporate handles incident response (different reporting mechanism, additional resolution steps), new methods for physical security (updated or new badging system), or new requirements dictated by company policy or Federal regulations. |
| Part c | The GDIT Training Department provides basic security awareness training to information system users (including managers, senior executives, and contractors), at least annually thereafter as part of the GDIT Corporate requirement: Annual Security Briefing Annual Information Security Awareness Culture of Responsibility The GDIT Corporate training department provides and tracks these courses through the myLMS online training system. GDIT Corporate automatically notifies individuals and their management chain of annual recurrence upcoming required training and any training which is overdue. Supplemental training not delivered through MyLMS is tracked by the ISSO using the training tracker, sign in sheets and individual Completion Certificates stored in the GDIT Cloud SharePoint training folder. Training materials (brown bag slide decks) are saved in the “Training” folder in techservices shared drive. |

### AT-3 Role-Based Security Training (L) (M) (H)

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

1. Before authorizing access to the information system or performing assigned duties;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| AT-3 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AT-3(c): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Per GDIT SEC-POL-IT-34 Security Awareness and Training, personnel that have significant information security roles and responsibilities are provided appropriate information system security training; (a) before authorizing access to the system or performing assigned duties; (b) when required by system changes; and (c) annually thereafter. The manager ensures that all new employees are given supervised on the job training in conjunction with the training required in the on-boarding process. In addition, a manager may assign specific training to employees through the MyLMS system that contains a library of training for any role in the GDIT Cloud. All employees who are involved with the architecture or management of the GDIT Information Security infrastructure receive a minimum of three security related training modules or courses annually. |
| Part b | Per GDIT SEC-POL-IT-34 Security Awareness and Training, personnel that have significant information security roles and responsibilities (such as those involved with the architecture or management of the GDIT Information Security infrastructure) are provided appropriate information system security training; (a) before authorizing access to the system or performing assigned duties; (b) when required by system changes; and (c) annually thereafter. System changes that could necessitate additional role-based training includes but is not limited to: Technology updates in existing systems; Technology changes in the system; and/or Additions to hardware or software. |
| Part c | The GDIT Training Department mandates and provides a minimum of three security related training modules or courses annual training to all GDIT Cloud employees who are involved with monitoring and maintaining the GDIT Cloud security infrastructure. As part of the annual employee assessment, managers use the IPC (goal setting) tool to identify training needs and document progress throughout the year. |

#### AT-4 Security Training Records (L) (M)

The organization:

1. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
2. Retains individual training records for [FedRAMP Assignment: at least one year].

| AT-4 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AT-4(b): at least one year | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AT-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud ISSOdocuments and monitors individual GDIT Cloud system securitytraining activities includingbasicsecurity awareness training and specificinformation system security training. The GDIT Cloud required minimum standards on securitytraining records are as follows: Training records for courses provided by GDIT corporate LMS training system are maintained by the GDIT training department. Newusers completethe GDIT Cloud Annual SecurityCertification Packet to confirm understandingof GDIT Cloud training and security requirements. The certification packet is signed on an annual basis by all GDIT Cloud \ personnel. The GDIT Cloud ISSOupdates the GDIT Cloud Training Tracker to reflect the completed training. The GDIT Corporate training department provides and tracks these courses through the myLMS online training system. GDIT Corporate automatically notifies individuals and their management chain of annual recurrence of upcoming required training and any training which is overdue. Supplemental training not delivered through MyLMS is tracked by the ISSO using the training tracker, sign in sheets and individual Completion Certificates stored in the GDIT Cloud SharePoint training folder. Training materials (brown bag slide decks) are saved in the “Training” folder on the techservices shared drive. |
| Part b | The GDIT Cloud ISSOretains training records in the GDIT Cloud SharePoint site for three (3) years from thedateof completion ofthetraining or when subsequent training has been updated. |

## Audit and Accountability (AU)

### AU-1 Audit and Accountability Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and
2. Reviews and updates the current:
   1. Audit and accountability policy [FedRAMP Assignment: at every 3 years]; and
   2. Audit and accountability procedures [FedRAMP Assignment: at least annually].

| AU-1 | Control Summary Information |
| --- | --- |
| Responsible Role: Information System Security Officer (ISSO) | |
| Parameter AU-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter AU-1(b)(1): every three years | |
| Parameter AU-1(b)(2): at least Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| AU-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.3. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, audit and accountability controls in the GDIT Cloud’s GDIT-OC-PRO-AU Audit and Accountability Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### AU-2 Audit Events (L) (M) (H)

The organization:

1. Determines that the information system is capable of auditing the following events: [FedRAMP Assignment: [Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes];
2. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
3. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
4. Determines that the following events are to be audited within the information system: [FedRAMP Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited continually for each identified event].

AU-2 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the JAB/AO.

| AU-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AU-2(a): a Parameter: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes | |
| Parameter AU-2(d): d Parameter: continually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager has determined that the following information system components as provided by the vendor are capable of auditing, at a minimum, the following events: Successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web Application, auditable events include: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes. Affected system components: CISCO Switch/Router CISCO ASA Firewall Cisco UCS Server Controller MS Windows OS MS Active Directory MS SQL Server Symantec EndPoint Protection AlienVault Traverse Red Hat NetApp OnCommand Unified Manager VMware vCenter RSA SecurID Appliance Ivanti Cherwell CISCO VPN The events for which the components generate audit logs are defined as part of AU-2d and configured as part of AU-12. |
| Part b | The Security Engineers coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events as follows: GDIT Cloud ISSO: Provides insight into the threat landscape and FedRAMP compliance. GDIT Cloud SOC Manager: Provides oversight on how the security analysts may respond to a particular event or series of events. GDIT Cloud System Administrators: Provides insight into the impact and/or level of effort to implement any auditing changes. GDIT Network Engineers: Provides insight into the impact and/or level of effort to implement any auditing changes. The selection of auditable events begins with the events that have been identified in component STIGs (see CM-6 part a) and events are added as needed based on intra-team collaboration (see above) and evolving threats. |
| Part c | The rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents is listed for each selected auditable event listed in AU-2a. as follows: Successful and unsuccessful account logon events Successful logon events provide a date/time stamp for who was on which system and can be valuable for determining when an incident occurred and who may have been responsible. Unsuccessful logon attempts can indicate a bruteforce attack or other attempts to gain unauthorized access. Account management events Attackers often attempt to change account privileges and/or create new accounts. Auditing these events can provide insight as to how an attacker accessed or attempted to access the system. Object access Auditing object access provides understanding about what systems or software may have been altered during an attack. Policy change An attacker may attempt a policy change to either loosen or restrict certain policies on the information system in order to facilitate the attack. Privilege functions All attackers attempt to escalate their own privilege on the system in order to gain access to more data and/or secure their persistence on the system. Understanding when privileged functions were invoked provides more information on what was done and when. Process tracking Certain processes may be stopped or started in order to facilitate an attack. An example would be an attacker stopping the process of antivirus software. System events These can provide insight on what an attacker did and when. If an attacker attempted to install something, it may show up on system events. For Web applications: All administrator activity Attackers always attempt to escalate their privileges when compromising a system. Tracking administrator activity can help in an investigation to determine what was done and when. Authentication checks These can be correlated with other logs to determine how an attacker breached or attempted to breach the system. Authorization checks These can be correlated with other logs to determine how an attacker breached or attempted to breach the system. Data deletions An attacker may attempt to cover his/her tracks by deleting data. Additionally, knowing when data was deleted can help in efforts to restore the application. Data access Understanding what data was accessed by an attacker or unauthorized user can help guide actions with regard to informing the appropriate parties in the event that PII was spilled. Data changes Understanding what changes were made to the data can help with the restoration process after an attack. Permission changes Permission changes can be an indicator of compromise or attempted compromise when the change were made without authorization. |
| Part d | The Security Engineers and the ISSO identify the audit events that are to be audited within the information system by reference to the STIGs and vendor hardening guides mentioned in CM-6. Those are community standards and justified by the publishers. In the event that no STIG or hardening guide is available for a technology, GDIT Cloud uses the events identified below: Cisco Switch/Router Login events Ethernet port status changes (up/down) ACL blocks Cisco ASA Firewall Login events Account management events Device configuration change Network access policy change Policy logging for “denied” traffic IDS logging for “alerts” Cisco UCS Server Controller Login events User account management Privilege functions System events Changes to Core system files (HIDS) MS Windows OS Login events User account management Privilege functions System events Changes to core system files (HIDS) MS Active Directory Login events User account management Privilege functions System events Access policy change Configuration policy change MS SQL Server Login events User account management Privilege functions System events Symantec Endpoint Protection Login events User account management Privilege functions System events Viruses/malware AlienVault Login events User account management Privilege functions System events Changes to core system files (HIDS) Traverse Login events User account management Privilege functions System events Red Hat Enterprise Linux Login events System events NetApp OnCommand Unified Manager Login events System events VMware vCenter Login events System events RSA SecureID Appliance Account management activities Login activities to the appliance administrative screens by administrative users Login activity for token holders to devices in the information system System events Ivanti Login events System events Whitelisting violations Cherwell Login events System events Cisco VPN Failed logins Successful/failed session connections Session disconnection These events are a subset of the auditable events listed in AU-2a. and are configured as part of control AU-12. |

### AU-3 Content of Audit Records (L) (M) (H)

The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

| AU-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-3 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud Network Engineers and System Administrators configure the GDIT Cloud to generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event. The GDIT Cloud auditing tools send all audit records to the GDIT Cloud MMS where they are processed, stored, and archived. The audit record details are described in the table below. Table 11-3. Auditable Data Contents |

### AU-4 Audit Storage Capacity (L) (M) (H)

The organization allocates audit record storage capacity in accordance with [Assignment: organization-defined audit record storage requirements].

| AU-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineer | |
| Parameter AU-4: 12 months of usage logs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-4 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### AU-5 Response to Audit Processing Failures (L) (M) (H)

The information system:

1. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and
2. Takes the following additional actions: [FedRAMP Assignment: organization-defined actions to be taken; (overwrite oldest record)].

| AU-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter AU-5(a): Security Engineer | |
| Parameter AU-5(b): low-impact: overwrite oldest audit records; moderate-impact: shut down | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Security Engineers have configured the GDIT Cloud MMS (Traverse) to notify both network and security analysts if any system’s audit functions fail within the GDIT Cloud. In addition to locally capturing audit data within the GDIT Cloud, all syslog data is also sent to the GDIT Cloud MMS SIEM for correlation and long-term storage. Should the network connection to the GDIT Cloud MMS SIEM be unavailable, the data is still available within the information system for forensic and audit purposes. Data flow will begin automatically once the network connection is re-established. |
| Part b | In the event of an audit processing failure, System Administrators shut down a failed component when audit processing fails. Then System Administrators restore a snap of the previous version of the component and processing continues. If the GDIT Cloud MMS SIEM logger fails, then the sensors buffer the data until such time as the GDIT Cloud MMS SIEM is initialized from a backup image. System administrators configure the system to automatically archive audit data within the GDIT Cloud in order to reduce the burden on individual systems and reduce the probability of audit failure. |

### AU-6 Audit Review, Analysis, and Reporting (L) (M) (H)

The organization:

1. Reviews and analyzes information system audit records [FedRAMP Assignment: at least weekly] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and
2. Reports findings to [Assignment: organization-defined personnel or roles].

AU-6 Additional FedRAMP Requirements and Guidance:

Requirement: Coordination between service provider and consumer shall be documented and accepted by the Authorizing Official. In multi-tenant environments, capability and means for providing review, analysis, and reporting to consumer for data pertaining to consumer shall be documented.

| AU-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analysts | |
| Parameter AU-6(a)-1: Continuously | |
| Parameter AU-6(a)-2: 2: organization-defined inappropriate or unusual activity:; Defined by AlienVault Correlation Directives described in the table below | |
| Parameter AU-6(b): GDIT Cloud Engineers | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Through the use of AlienVault Correlation Directives, the Security Analysts review audit logs continuously for inappropriate or unusual activity. The table below lists and describes the various AlienVault Correlation Directives that are used to detect inappropriate or unusual activity: The review is performed using the AlienVault tool to identify instances of inappropriate or unusual activity. AlienVault automatically and in near real time correlates and analyzes the log records using correlation directives in which there are over 3,000 correlation rules. Updates to the correlation rules are provided by AlienVault. Security Operations receives alerts and reviews the relevant information. Security Analysts record the alerts and resolutions as events in the ticketing system. Events may be dismissed as false positives, authorized, or turned into incidents in the ticketing system. The response to incidents is described in IR-4 Incident Response within this document. |
| Part b | The Security Analysts report the results of the review of AlienVault Incidents and Events of interest at the weekly GDIT Cloud SOC team meeting. The findings are added to the meeting minutes and kept on the secure GDIT Cloud techservices Shared Drive. |

### AU-8 Time Stamps (L) (M) (H)

The information system:

1. Uses internal system clocks to generate time stamps for audit records; and
2. Records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets [Assignment: one second granularity of time measurement].

| AU-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter AU-8(b): HH:MM:SS | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | System and Network Administrators ensure that GDIT Cloud system components are configured to use internal system clocks to generate time stamps for audit records. It should be noted that all modern operating systems timestamp their logs as a Common Criteria requirement. |
| Part b | System and Network administrators have configured all information system components to use UTC for the system clock rather than a specific time zone. The appropriate engineer sets each device to coordinate the time with the NTP servers. The level of granularity for internal system clocks is at a minimum HH:MM:SS, which is inherent in each OS in the environment. Some applications display time in local zones using an offset, but this does not affect logging records. |

### AU-9 Protection of Audit Information (L) (M) (H)

The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

| AU-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-9 What is the solution and how is it implemented? |
| --- |
| The System Manager protects audit information and audit tools from unauthorized access, modification, and deletion through strict access control definitions stated in Appendix 10: the Roles and Privileges Matrix. Consequently, the GDIT Cloud access control AD configuration restricts local audit logs to admin only access, which protects against unauthorized access, as follows: Authorized personnel are limited to the SOC Analyst role and SOC Administrator Group defined in AD. In addition, each device Administrator has access to local audit logs of the device. See AU-2 for additional details. Only authorized personnel with a valid named account and RSA token are authorized for logical access to GDIT Cloud’s audit record system (AlienVault). Security credentials are reviewed on the RSA appliance every 90 days. All audit logs are sent continuously, at the time of the event to an AlienVault logger that is only accessed by security personnel. See AU-2 for additional details. |

### AU-11 Audit Record Retention (L) (M)

The organization retains audit records for [FedRAMP Assignment: at least ninety (90) days] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

AU-11 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider retains audit records on-line for at least ninety days and further preserves audit records off-line for a period that is in accordance with NARA requirements

| AU-11 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter AU-11: at least ninety days | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-11 What is the solution and how is it implemented? |
| --- |
| Security Engineers configure the Cloud MMS SIEM to retain audit events for a minimum period of one year to support after-the-fact investigation of security incidents. Currently, the data within the logger in AlienVault is set to never expire. So, in effect, GDIT Cloud will keep the data for greater than one year. Logger data is backed up (copied separately) in weekly increments to a storage server. This will also pertain to AU-5b, as logger data can then be restored to the logger if the need arises. |

### AU-12 Audit Generation (L) (M) (H)

The information system:

1. Provides audit record generation capability for the auditable events defined in AU-2 a. at [FedRAMP Assignment: all information system components where audit capability is deployed/available];
2. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and
3. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3.

| AU-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter AU-12(a): all information system components where audit capability is deployed | |
| Parameter AU-12(b): ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| AU-12 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Security Engineers configure AlienVault to generate and store audit records in accordance with contents listed and defined in AU-2 and AU-3. |
| Part b | The System Manager allows the Security Engineers to select which auditable events are to be audited by specific components of the information system. |
| Part c | The events (Part a) that are configured by the Security Engineers (Part b) are stored locally and sent to the GDIT Cloud MMS SIEM for processing and storage. Updates to the audited events are made as part of the review requirement in AU-2(3) if needed. Changes to component auditing capabilities are treated as any other change and fall under the Change Management process outlined in the CM family of controls. |

## Security Assessment and Authorization (CA)

### CA-1 Certification, Authorization, Security Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and
2. Reviews and updates the current:
   1. Security assessment and authorization policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Security assessment and authorization procedures [FedRAMP Assignment: at least annually].

| CA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter CA-1(b)(1): at least every three years | |
| Parameter CA-1(b)(2): Assignment: at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.4. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, security assessment and authorization controls in the GDIT Cloud’s GDIT-OC-PRO-CA Security Assessment and Authorization Procedures. The policy and procedures documents are stored in the secure GDIT Cloud SharePoint site, which maintains change history and version control. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### CA-2 Security Assessments (L) (M) (H)

The organization:

1. Develops a security assessment plan that describes the scope of the assessment including:
   1. Security controls and control enhancements under assessment;
   2. Assessment procedures to be used to determine security control effectiveness; and
   3. Assessment environment, assessment team, and assessment roles and responsibilities;
2. Assesses the security controls in the information system and its environment of operation [FedRAMP Assignment: at least annually] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;
3. Produces a security assessment report that documents the results of the assessment; and
4. Provides the results of the security control assessment to [FedRAMP Assignment: individuals or roles to include the FedRAMP Program Management Office (PMO)].

CA-2 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Annual Assessment Guidance

https://www.fedramp.gov/documents/

| CA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-2(b): at least annually | |
| Parameter CA-2(d): PMO ISSO and GDIT ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| CA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | To conduct impartial security assessments, the GDIT Cloud System Owner partners with a FedRAMP certified Third Party Assessment Organization (3PAO), to develop a security assessment plan. The 3PAO is responsible for developing the Security Assessment Plan (SAP) that describes the scope of the assessment including: Security controls and control enhancements under assessment Assessment procedures to be used to determine security control effectiveness Assessment environment, assessment team, and assessment roles and responsibilities The 3PAO creates a plan using the FedRAMP SAP template. The SAP identifies all the assets within the scope of the assessment, including components such as hardware, software, and physical facilities. It also provides a roadmap and methodology for execution of the tests and indicates that they will use the FedRAMP associated security test cases that are provided in the form of a worksheet. Once completed, the 3PAO submits the SAP to the FedRAMP PMO for approval in the timeline dictated by the PMO for reaccreditation. |
| Part b | GDIT contracts an approved 3PAO to conduct the assessment on a schedule dictated by the FedRAMP PMO office, currently on an annual basis determined by the anniversary of the initial P-ATO. The 3PAO assesses the security controls dictated in the Security Assessment Plan (SAP) and previously approved by the FedRAMP PMO, as they are implemented in the in the GDIT Cloud. The assessment determines the extent to which the controls are implemented correctly, operating as intended, and produce the desired outcome with respect to meeting the security requirements for the system. The 3PAO assesses the security controls in the GDIT Cloud for the initial authorization and (then annually thereafter) to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The 3PAO performs the testing of the GDIT Cloud by following the procedures detailed in the SAP and in accordance with the test case procedures. As part of the continuous monitoring program and to satisfy annual testing requirements, the 3PAO will review the GDIT Cloud documented controls to assess all applicable controls for a moderate system during a three-year cycle based on a 1/3rd scheme; that is, during each annual assessment a review of 1/3rd of the controls shall take place. |
| Part c | The 3PAO produces a security assessment report (SAR) that documents the results of the assessment using the FedRAMP PMO provided template. The purpose of this document is to provide the system owner and the cloud service provider (CSP) a security assessment on a cloud system that evaluates the system's implementation of, and compliance with, the FedRAMP baseline security controls. The implementation of security controls is described in the System Security Plan, and required by FedRAMP to meet Federal Information Security Management Act (FISMA) compliance mandates |
| Part d | The 3PAO provides the results of the security assessment to GDIT, the FedRAMP PMO, and the FedRAMP Joint Advisory Board (JAB) using the FedRAMP PMO provided Security Assessment Report (SAR) template. This report includes recommendation of Authorization to Operate . The 3PAO produces both a written report as well as an oral slide presentation, delivered to the panels dictated by the FedRAMP PMO. The GDIT Cloud SAP/SAR and the GDIT Cloud authorization statement are then assembled into a complete GDIT Cloud A&A package, which is provided to the GDIT Cloud ISSO and GDIT ISSO for review and submission to the FedRAMP JAB. |

#### CA-2 (1) Control Enhancement (L) (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.

CA-2 (1) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB Authorization, must use an accredited Third Party Assessment Organization (3PAO).

| CA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: GDIT Cloud ISSO | |
| Parameter CA-2(1): Independent | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-2 (1) What is the solution and how is it implemented? |
| --- |
| The GDIT System Owner employs an independent assessor to perform an assessment of the GDIT Cloud. GDIT selects this Third Party Assessment Organization (3PAO) from the list of accredited 3PAOs supplied by the FedRAMP PMO. The 3PAO: Develops a security assessment plan (SAP) Assesses the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements Produces a Security Assessment Report (SAR) that documents the results of the assessment Provides the results of the security control assessment, in writing, to the FedRAMP JAB. |

### CA-3 System Interconnections (L) (M) (H)

The organization:

1. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements;
2. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
3. Reviews and updates Interconnection Security Agreements [FedRAMP Assignment: at least annually and on input from FedRAMP].

Table 13‑3. CA-3 Authorized Connections

| Authorized Connections Information System Name | Name of Organization PITG System Connects To | Role and Name of Person Who Signed Connection Agreement | Name and Date of Interconnection Agreement |
| --- | --- | --- | --- |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |
| <Authorized Connections System Name> | <Name Org CSP System Connects To> | <Role and Name Signed Connection Agreement> | <Name and Date of Interconnection Agreement> |

| CA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-3(c): 3 years / annually and on input from FedRAMP | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO authorizes an Interconnection Security Agreement to document connections from the information system to external information systems. See section 10 for information about implementation details. |
| Part b | The ISSO documents for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated in the Interconnect Security Agreement. |
| Part c | The ISSO reviews and updates Interconnection Security Agreements annually on the anniversary of the agreements approval, or upon input from the FedRAMP PMO. The ISSO reviews ISAs in conjunction with the annual review of the System Security Plan. |

### CA-5 Plan of Action and Milestones (L) (M) (H)

The organization:

1. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and
2. Updates existing plan of action and milestones [FedRAMP Assignment: at least monthly] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

CA-5 Additional FedRAMP Requirements and Guidance:

Requirement: Plan of Action & Milestones (POA&M) must be provided at least monthly.

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Plan of Action and Milestones (POA&M) Template Completion Guide

<https://www.fedramp.gov/documents/>

| CA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-5(b): at least monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | On a monthly schedule dictated by the FedRAMP PMO, the ISSO maintains the POA&M tracker by updating tracking information related to all vulnerability and audit findings. Each entry tracks a unique finding, and includes its name, a description, the source used to detect the vulnerability, the assets involved, a remediation plan, the date detected, planned milestones and remediation dates, and the status of and requests for deviation from standard policy. At a minimum, items dependent on vendor interaction must be updated on a monthly basis. Resolved items are removed from the open items tracker while newly discovered items create new line items in the tracker. The POA&M tracker contains the following headings (as required by FedRAMP): |
| Part b | The GDIT Cloud ISSO reviews and updates the GDIT Cloud POA&M at least monthly to ensure that it is in compliance with the FedRAMP standards and delivered to the FedRAMP PMO via MAX.gov. As a weakness or deficiency is identified, the ISSO creates a unique ticket in the ticket system for tracking through its lifecycle and documents the ticket in the POA&M tracker. During monthly updates, the ISSO validates each POA&M line item against raw assessment scan data, maintenance activity, and configuration changes documented within those POA&M tickets. The ISSO updates all fields of the template as prescribed in the FedRAMP POA&M Template guidance. |

### CA-6 Security Authorization (L) (M) (H)

The organization:

1. Assigns a senior-level executive or manager as the authorizing official for the information system;
2. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and
3. Updates the security authorization [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs].

CA-6c Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F ([SP 800-37](http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf)). The service provider describes the types of changes to the information system or the environment of operations that would impact the risk posture. The types of changes are approved and accepted by the JAB/AO.

| CA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-6(c): every three years or when a significant change occurs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | As a FedRAMP system, the authorization official for GDIT Cloud is the Joint Authorization Board (JAB). |
| Part b | Before commencing operations of the information system or addition of any subcomponents, the JAB is made aware of, and authorizes its use. Before a change is implemented the ISSO evaluates the change request for applicability to the NIST SP800-37 Rev1 Appendix F criteria for definition of a "Significant Change." In accordance with FedRAMP PMO guidance, those changes meeting the NIST requirements are briefed to the PMO for further determination on approval by the JAB. With JAB approval, the Significant Change is permitted to proceed to the Change Advisory Board (CAB). The AO bases this decision for authorization on the voting charter members of the CAB, the documentation of the change request ticket, and the assessment of the technology owner implementing the change. The Configuration-Change Manager documents this authorization during meeting minutes and in individual change requests tickets. |
| Part c | The ISSO works with the FedRAMP PMO and establishes an annual schedule for the procedure of the update and re-assessment of the security authorization. The milestones established by the FedRAMP PMO ensure a thorough evaluation of the system. The assessment is accomplished on an annual basis as determined by the anniversary of the initial Provisional Authorization to Operate (P-ATO), or as otherwise determined by the FedRAMP PMO. The P-ATO for the GDIT Cloud is updated at least every three years or when a significant change occurs as defined by the Change Management process. |

### CA-7 Continuous Monitoring (L) (M) (H)

The organization develops a continuous monitoring strategy and implements a continuous monitoring program that includes:

1. Establishment of [Assignment: organization-defined metrics] to be monitored;
2. Establishment of [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessments supporting such monitoring;
3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;
4. Ongoing security status monitoring of organization-defined metrics in accordance with the organizational continuous monitoring strategy;
5. Correlation and analysis of security-related information generated by assessments and monitoring;
6. Response actions to address results of the analysis of security-related information; and
7. Reporting the security status of organization and the information system to [FedRAMP Assignment: to meet Federal and FedRAMP requirements] [Assignment: organization-defined frequency].

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement: Operating System Scans: at least monthly. Database and Web Application Scans: at least monthly. All scans performed by Independent Assessor: at least annually.

Guidance: CSPs must provide evidence of closure and remediation of a high vulnerability within the timeframe for standard POA&M updates.

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Continuous Monitoring Strategy Guide

<https://www.FedRAMP.gov/documents/>

| CA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-7(a): organization-defined metrics | |
| Parameter CA-7(b)-1: organization-defined frequencies | |
| Parameter CA-7(b)-2: organization-defined frequencies | |
| Parameter CA-7(g)-1: to meet Federal and FedRAMP requirements | |
| Parameter CA-7(g)-2: organization-defined frequency | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO establishes metrics to be monitored in the Continuous Monitoring Plan. The GDIT Cloud implements a Continuous monitoring program consistent with the direction published by the FedRAMP PMO in the Continuous Monitoring Strategy Guide. The metrics described in this guide are extensive and include but are not limited to, the number of raw vulnerabilities by their severity (H, M, L), associated with operating systems, databases, and web applications, the number of POA&M items and their duration of exposed risk, and the number of Deviation Requests including operational requirements and vendor dependencies. The GDIT Cloud ISSO ensures that the minimally required controls and frequencies as outlined in Appendix A Table A-1 of Continuous Monitoring Strategy Guide are identified as metrics for continuous monitoring, specifically, items identified as follows (indicated by row numbers as listed in the Strategy Guide): Row 3: CM-8(3) Measure: Amount of time to detect new assets. Standard: 5 minutes or less Row 4: IR-6 Measure: Time between the discovery of an incident until the incident is reported to FedRAMP PMO. Standard: Timelines outlined by US-CERT: http://www.us-cert.gov/government-users/reporting-requirements Row 8: CP-3a Measure: Amount of time (days) between when a person assumes a contingency role and when they receive role-based contingency training. Standard: 10 days or less Row 10: RA-5d Measure: Amount of time (in days) between the discovery of a vulnerability and the remediation of the same. Standards: High Risk: 30 days or less Moderate Risk: 90 days or less Low Risk: 180 days or less Row 12: PE-8b Measure: Frequency of visitor access records Standard: Monthly Note: This is a subset of the total controls selected for continuous monitoring. See Part b for the list of controls and frequencies. |
| Part b | The ISSO establishes the frequency for monitoring and frequency for assessments supporting such monitoring in the Continuous Monitoring Plan. The GDIT Cloud monitors and performs assessments of the metrics of the ConMon program on a monthly basis consistent with delivery of FedRAMP PMO deliverable products. Visibility of this monthly ConMon cycle is maintained weekly by the ISSO in the weekly ISSO meeting with bimonthly briefings to the System Owner. The following are the controls and frequencies for continuous monitoring activities: |
| Part c | The GDIT Cloud information system is assessed by the 3PAO on an annual basis. The 3PAO produces a Security Assessment Plan, which must be approved by the JAB prior to testing. Following the testing, the 3PAO produces a Security Assessment Report (SAR). This testing is conducted at least annually or when there is a significant change to the system. |
| Part d | The ISSO performs ongoing security status monitoring of the metrics defined in section a of this control. Cherwell tickets are generated to maintain tracked visitor logs, security incidents, new assets, security incidents and resolution, vulnerabilities, and POA&Ms. Training completion records are stored in SharePoint. |
| Part e | The ISSO with the security team performs correlation and analysis of security-related information generated by assessments and monitoring to produce a remediation strategy that becomes a CR if a change is needed to the system. The ISSO also takes the information provided by the 3PAO in the SAR and generates POA&M items for remediation, tracking, and reporting purposes. Other findings from continuous monitoring activities are either remediated immediately if possible or added to the POA&M list. The POA&M list allows the ISSO to see all relevant system vulnerabilities and risks in one place, making it easier to correlate and analyze the security-related information. |
| Part f | The GDIT ISSO works with the System Owner to prioritize resources dedicated to response actions following analysis of security findings. With visibility of the overall status of the IS, the ISSO categorizes risks and the remediation efforts in order to achieve the greatest reduction of overall risk as quickly as possible. If a finding cannot be remediated immediately, the ISSO works with the System Owner to assess impact, coordinate resources, and devise a plan for remediation. The item is added to the POA&M list to be reported to the FedRAMP PMO monthly and tracked and remediated in accordance with the risk levels and timelines established in RA-5. |
| Part g | The ISSO reports the security status to FedRAMP of the GDIT Cloud in the monthly POA&M and inventory update. This monthly reporting activity provides detailed tracking and monitoring of vulnerabilities along with raw scan reports. The 3PAO provides the Security Assessment Report (SAR) to FedRAMP on an annual basis. |

CA-7 Additional FedRAMP Requirements and Guidance:

Requirement 1: Operating System Scans: at least monthly

Requirement 2: Database and Web Application Scans: at least monthly

Requirement 3: All scans performed by Independent Assessor: at least annually

| CA-7 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Req. 1 According to the Security Calendar, the Security Team conducts Operating System Scans at least monthly using Tenable Security Center. Knowledge Article KA 11038, Reference: FedRAMP Boundary – IP Address Subnets, in Cherwell defines the IS boundary IP address range. The Security Engineer maintains the profile for vulnerability scans according to that boundary definition in the KA. The Security Analyst schedules the scanner to automatically conduct scans at least once a month. The ISSO analyses the results of these scans and reviews the analysis in a weekly ISSO meeting with the Security Manager. The results of the analysis and follow-up actions are recorded in the ISSO meeting minutes and uploaded to the secure SharePoint portal. See CA-7 parts e, f, and g above for details on correlation and analysis, response actions, and status reporting. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-7 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Req. 2 The Security Analyst conducts Database and Web Application Scans at least monthly. The scans are conducted manually by accessing the tool and initiating the scan activity. The GDIT Cloud MMS employs Security Content Automation Protocol (SCAP) commercial-off-the-shelf (COTS) vulnerability scanning tools that include the capability to readily update the list of vulnerabilities scanned. See the table below for a list of tools used for vulnerability scanning and their purpose: See CA-7 parts e, f, and g above for details on correlation and analysis, response actions, and status reporting. |
| Req. 2 | Req. 3 The 3PAO (independent assessor) conducts full scans at least annually. The 3PAO assesses the security controls dictated in the Security Assessment Plan (SAP) and previously approved by the FedRAMP PMO, as they are implemented in the in the GDIT Cloud. |
| Req. 3 | Click or tap here to enter text. |

### CA-9 Internal System Connections (L) (M) (H)

The organization:

1. Authorizes internal connections of [Assignment: organization-defined information system components or classes of components] to the information system; and
2. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

| CA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CA-9(a): organization-defined information system components or classes of components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Internal connections of new systems in GDIT Cloud would necessarily fall under the Change management process, since it is a system change. Accordingly, he System Manager authorizes internal connections of the GDIT Cloud through the review and approval of the GDIT Cloud change management process governed by the GDIT Cloud Change Management Process and Procedures Guide. The classes of components covered in this control are as follows: Networking components (routers, switches) Firewalls Storage components (the addition of physical storage) Appliances Other hardware connections (UCS chassis) Cloud laptops (as a group rather than individually) Other mobile devices (not applicable at this time) Wireless access points (not applicable at this time) |
| Part b | The Network Engineer documents all internal connections, the interface characteristics, security requirements, and the nature of the information communicated through the Network Architecture diagrams that are approved by the CAB. The GDIT Architectural layout in Section 8.4 of this SSP documents the internal connections of the information system. |

## Configuration Management (CM)

### CM-1 Configuration Management Policies and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
2. Reviews and updates the current:
   1. Configuration management policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Configuration management procedures [FedRAMP Assignment: at least annually].

| CM-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CM-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter CM-1(b)(1): at least every 3 years | |
| Parameter CM-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CM-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.5. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, configuration management policy and associated access controls in the GDIT Cloud’s GDIT-OC-PRO-CM Configuration Management Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### CM-2 Baseline Configuration (L) (M) (H)

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

| CM-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Configuration-Change Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-2 What is the solution and how is it implemented? |
| --- |
| The Configuration-Change Manager provides an initial system baseline configuration as defined by the CM Plan: The GDIT Cloud Service Asset and Configuration Management Process and Procedures Guide. The GDIT Cloud baseline configuration is maintained by processes defined in the Guide. Configuration management enables the organization to manage the IT infrastructure baseline. The baseline is updated when a change is implemented into Production or restored if a release in Production fails. Changes to the baseline are systematically monitored and controlled within the version control, change management, and configuration auditing functions. The configuration baseline repository is the Cherwell CMDB that contains Configuration Item (CI) reference information that identifies the official baseline of the environment. Baselines serve as the foundation for 3PAO testing with DISA STIGs being used for security configuration baselines. If changes are made during 3PAO testing, the implementation team follows normal Change Management as dictated in the GDIT Cloud Change Management Process and Procedures Guide. All changes to the operational system are approved by the change management process that requires CAB approval. Furthermore, changes to the operational system must follow the SDLC that mandates a test phase before proceeding to implementation. (See CM-3 (2).) However, during 3PAO testing, the CAB process will be modified to consider the impact to 3PAO testing. If the proposed change impacts 3PAO testing or invalidates a previous 3PAO test, the 3PAO will be notified. See Section 9 for a list of hardware, software, and network baseline components. |

### CM-4 Security Impact Analysis (L) (M) (H)

The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

| CM-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analysts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-4 What is the solution and how is it implemented? |
| --- |
|  |

### CM-6 Configuration Settings (L) (M) (H)

The organization:

1. Establishes and documents configuration settings for information technology products employed within the information system using [FedRAMP Assignment: see CM-6(a) Additional FedRAMP Requirements and Guidance] that reflect the most restrictive mode consistent with operational requirements;

CM-6(a) Additional FedRAMP Requirements and Guidance:

Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) (<http://scap.nist.gov/>) validated or SCAP compatible (if validated checklists are not available).

Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>.

1. Implements the configuration settings;
2. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and
3. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

| CM-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter CM-6(a)-1: ; Requirement 1: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish configuration settings or establishes its own configuration settings if USGCB is not available.; Requirement 2: The service provider shall ensure that checklists for configuration settings are Security Content Automation Protocol (SCAP) validated or SCAP compatible (if validated checklists are not available). | |
| Parameter CM-6(a)-2: GDIT Cloud system components | |
| Parameter CM-6(c)-1: ; For Windows servers:; GPO settings are applied to the server. Once the settings are confirmed in place, a Tripwire scan is run against the server to verify that it passes the required configuration checks and discrepancies are remediated.; For Linux servers and all network or storage devices:; The STIG requirements are manually implemented against the device. Once the settings are confirmed in place, a Tripwire scan is run against the server to verify that it passes the required configuration checks and discrepancies are remediated.; | |
| Parameter CM-6(c)-2: The following roles establishes and documents configuration settings for information technology products employed within the GDIT Cloud: If there is a new technology deployed to the environment, the ISSO validates if there is a valid STIG for that technology. If so, GDIT Cloud implements that STIG. If not, the ISSO selects other configuration guidance from another organization (e.g., CIS) or from the vendor. The Technology owner identifies required deviations and communicates them to the ISSO, who is responsible for approving or denying. The ISSO periodically views the latest STIGs and determines if a new one needs to be analyzed and applied to the respective technology. As an enhancement to USGCB standards and as required by the customers of the GDIT Cloud, the configuration settings of DISA STIGs establish system configuration standards, when applicable. The system components are measured and validated against Tripwire policies during a periodic scan (as defined in CM-6(1)) of the system. The policies that Tripwire uses are based on settings provided by the respective STIG settings. As STIGs are updated by DoD, Tripwire updates the policies to reflect the new settings if applicable. The Security Engineer downloads and applies the rulesets and applicable tests to meet STIG configurations from the Tripwire User Portal as they are published by the vendor. Vendor publication does not occur more than quarterly. Table 11-6 below outlines the STIGs that have been selected for each technology. Table 11-6. Configuration Standards | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| CM-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The appropriate technology engineer implements the configuration settings, as follows: For Windows servers: For most STIG configuration settings in the Windows environment, the Windows Engineer applies settings to servers in the domain through the use of Domain Group Policy Objects (GPO). Configurations unable to be applied through the domain policy are configured manually on individual systems. The Security Engineer executes Tripwire scans following maintenance and at least weekly to validate that it meets the STIG requirements. For Linux servers and all network or storage devices: The Linux Engineer applies some standard configuration through the Centrify Configuration Manager module of the Active Directory. The Linux Engineer manually implements the STIG configurations unable to be applied through Centrify. The Security Engineer executes Tripwire scans following maintenance and at least weekly to validate that it meets the STIG requirements. For Infrastructure devices: The Network Engineer applies all network configurations directly to infrastructure systems. The Security Engineer executes Tripwire scans following maintenance and at least weekly to validate that it meets the STIG requirements. |
| Part b | The process for identifying, documenting, and approving any deviations from established configuration settings is governed by the compliance exception process as described in KA 10794, Compliance Exception Procedure. The steps involved in the above KA are as follows: Identify: The Technology Owner identifies required deviations and communicates them to the ISSO who is responsible for approving or denying. Approve: The ISSO who is responsible for approving or denying. Document: The Security Engineers implement waivers in Tripwire and annotate the approval provided by the ISSO. Justify: The requester provides a justification for the non-compliance of the specific setting. Reasons for exceptions are consistent with FedRAMP deviation requests regarding vulnerabilities as follows: 1) Operational Requirement: the setting cannot be configured without negatively impacting the operation of the system; 2) False Positive: the setting has been applied but is still appearing as a finding in the Tripwire report or the setting is not applicable to the system component (cannot be applied). This process dictates the approval procedure and artifacts necessary to document an exception to the STIG configuration as well as recurring review requirements and includes the following procedures. The change of configuration is governed by the GDIT Cloud Change Management Process and Procedures Guide, which includes the deviation request and approval from the FedRAMP PMO. The GDIT Cloud Engineering Team reviews changes and updates the baseline configuration stored in the Cherwell ticketing system where required for operational or service delivery reasons. |
| Part c | The GDIT Cloud personnel monitor and control changes to the configuration settings in accordance with organizational policies and procedures, as follows: Monitoring of configuration settings is conducted as follows: Tripwire automatically runs configuration scans of all components in the GDIT Cloud IaaS. The scans compare the settings applied to each component with the policy established in Tripwire (see Table 11-6). If the component setting is consistent with the policy the report shows the component setting as “green” compliant. If the component setting is not consistent with the policy—deviations notwithstanding. See CM-6 part c—the Tripwire report shows the setting as “red” non-compliant. The scans are automatically run daily and reports are automatically sent by the Tripwire system to the ISSO and the specific technology owners. This allows configuration settings to be monitored. GDIT Cloud Configuration-Change Manager controls changes to the configuration settings in accordance with the GDIT Cloud Change Management Process and Procedures Guide. Controlling Changes to Configuration Settings The authorized change process is documented in CM-3 . |
| Part d | Click or tap here to enter text. |

### CM-7 Least Functionality (L) (M) (H)

The organization:

1. Configures the information system to provide only essential capabilities; and
2. Prohibits or restricts the use of the following functions, ports, protocols, and/or services [FedRAMP Assignment: United States Government Configuration Baseline (USGCB)]

CM-7 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall use the Center for Internet Security guidelines (Level 1) to establish list of prohibited or restricted functions, ports, protocols, and/or services or establishes its own list of prohibited or restricted functions, ports, protocols, and/or services if USGCB is not available. If no recognized USGCB is available for the technology in use, the CSP should create their own baseline and include a justification statement as to how they came up with the baseline configuration settings.

Guidance: Information on the USGCB checklists can be found at: <https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline>

Partially derived from AC-17 (8).

| CM-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter CM-7(b): Organization-defined list of allowed functions, ports, protocols, and/or services are found in Table 10-4 | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization, | |

| CM-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Click or tap here to enter text. |
| Part b | Click or tap here to enter text. |

### CM-8 Information System Component Inventory (L) (M) (H)

The organization:

1. Develops and documents an inventory of information system components that:
   1. Accurately reflects the current information system;
   2. Includes all components within the authorization boundary of the information system;
   3. Is at the level of granularity deemed necessary for tracking and reporting; and
   4. Includes [Assignment: organization-defined information deemed necessary to achieve effective information system component accountability]; and
2. Reviews and updates the information system component inventory [FedRAMP Assignment: at least monthly].

CM-8 Additional FedRAMP Requirements and Guidance:

Requirement: Must be provided at least monthly or when there is a change.

| CM-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Configuration-Change Manager | |
| Parameter CM-8(a)(4): The service provider defines information deemed necessary to achieve effective property accountability: hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address Property accountability information is approved and accepted by the JAB. | |
| Parameter CM-8(b): At least Monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Configuration-Change Manager develops and documents an inventory of information system components that accurately reflects the current information system through the CMDB that is kept in Cherwell. Whenever there is a change to the inventory, the CMDB is updated. The CMDB contains all of the Configuration Items (CIs) associated with the GDIT Cloud system boundary. Section 9.1 of this document lists the current Hardware Inventory Section 9.2 of this document lists the current Software Inventory Section 9.3 of this document lists the current Network Inventory The organization develops, documents, and maintains an inventory of information system components that is at the level of granularity deemed necessary for tracking, reporting, and accountability as defined in the GDIT Cloud Service Asset and Configuration Management Process and Procedures Guide. CI attributes in the CMDB deemed necessary to achieve accountability are as follows: |
| Part b | The Configuration-Change Manager reviews and updates the component inventory on a monthly basis. For VMs: Discrepancies verified between the CMDB and vCenter based on SQL comparison. Any discrepancies are researched and validated with the appropriate team(s). Resulting changes are then made to the CMDB following KA 10782 How To: Update the CMDB using the CI Template. For Hardware: Discrepancies verified between the CMDB and Tripwire and IFS based on SQL comparison. Any discrepancies are researched and validated with the appropriate team(s). Resulting changes are then made to the CMDB following KA 11638. For Software: Discrepancies verified between the CMDB and Ivanti based on SQL comparison. Any discrepancies are researched and validated with the appropriate team(s). Resulting changes are then made to the CMDB. |

### CM-10 Software Usage Restrictions (L) (M) (H)

The organization:

1. Uses software and associated documentation in accordance with contract agreements and copyright laws;
2. Tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
3. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

| CM-10 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager determines that GDIT Cloud personnel use of software and associated documentation must be in accordance with contract agreements and copyright laws as stated in the GDIT Cloud Rules of Behavior that each person must sign as part of being granted access to the system. Additionally, all software is tracked as a configuration item (CI) as stated in The Asset & Configuration Management Process and Procedures Guide (2/4/2015) , section 3.2. |
| Part b | The Configuration-Change Manager tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution through the license management process as follows: The GDIT Asset Manager tracks the new procurements and licenses and provides a monthly report License procurement and lifecycle dates are stored in the CMDB The NOC runs a scan of the environment using Ivanti and The Configuration-Change Manager compares the scan results against the CMDB and then the updates the CMDB accordingly. Techservices utilizes Ivanti and Traverse to send email alerts prior to one month of license expiration. |
| Part c | The System Manager determines that the use of peer-to-peer file sharing technology is not allowed by GDIT Cloud personnel as stated in the GDIT Cloud Rules of Behavior, that each person must sign as part of being granted access to the system. Further, any request for additional software must go through the change control process, be approved, and then the software must be added to the Ivanti whitelist in order for the software to execute on the system. If a peer-to-peer file sharing technology were attempted to be installed on the system, automatic controls would prevent it from executing. |

### CM-11 User-Installed Software (L) (M) (H)

The organization:

1. Establishes [Assignment: organization-defined policies] governing the installation of software by users;
2. Enforces software installation policies through [Assignment: organization-defined methods]; and
3. Monitors policy compliance [FedRAMP Assignment: Continuously (via CM-7 (5))].

| CM-11 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CM-11(a): policies in Rules of Behavior | |
| Parameter CM-11(b): monitoring for illegal system usage or atypical behavior. | |
| Parameter CM-11(c): Continuously Monitoring | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CM-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager and ISSO establish policies governing the installation of software by users in the GDIT Cloud Rules of Behavior , standard users are not permitted to install any software on any system. Administrators are permitted to install software related to their role only in accordance with Change Management procedures and the SDLC. |
| Part b | The information system employs certificate signed software whitelisting through Ivanti Application Control to deny-by-default, approve-by-exception, the execution of installed components on Windows operating systems. As the application operates at the kernel level, software not approved to execute in the information system is halted before entering memory. Cisco, ESXi, NetApp, and other appliances have no mechanism for user applied software. RHEL servers do not fall under the protection of Ivanti, however, they are monitored by Security Analysts using the SIEM solution, which provides alerting in the event that software is installed on the server(s). Access to RHEL servers is restricted to administrators only. |
| Part c | Ivanti provides monitoring of policy compliance by restricting the installation of software not contained on the approved whitelist. Ivanti Application Control will cause the installation to fail until it has been approved through a Service Request and the NOC updates the whitelist. Logs of software installations on both Windows and RHEL servers are recorded within the SIEM AlienVault. |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls; and
2. Reviews and updates the current:
   1. Contingency planning policy [FedRAMP Assignment: at least every three (3) years].; and
   2. Contingency planning procedures [FedRAMP Assignment: at least annually].

| CP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CP-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter CP-1(b)(1): at least every three years | |
| Parameter CP-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| CP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s contingency plan policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.6. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, contingency planning policy and associated controls in the GDIT Cloud’s GDIT-OC-PRO-CP, Contingency Planning Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### CP-2 Contingency Plan (L) (M) (H)

The organization:

1. Develops a contingency plan for the information system that:
   1. Identifies essential missions and business functions and associated contingency requirements;
   2. Provides recovery objectives, restoration priorities, and metrics;
   3. Addresses contingency roles, responsibilities, assigned individuals with contact information;
   4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
   5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and
   6. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
3. Coordinates contingency planning activities with incident handling activities;
4. Reviews the contingency plan for the information system [FedRAMP Assignment: at least annually];
5. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
6. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and
7. Protects the contingency plan from unauthorized disclosure and modification.

CP-2 Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations the contingency lists include designated FedRAMP personnel.

| CP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CP-2(a)(6): .(6) ISSO, Cloud System Manager | |
| Parameter CP-2(b): key personnel defined in Appendix A of the CP | |
| Parameter CP-2(d): at least annually | |
| Parameter CP-2(f): key personnel defined in Appendix A of the CP | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager has developed the GDIT Cloud IT Contingency Plan as a deliverable that is part of the SSP (Attachment 6). The document contains: Identifies essential missions and business functions and associated contingency requirements (Appendix L) Provides recovery objectives, restoration priorities, and metrics (Section 1.4 and Appendix L) Addresses contingency roles, responsibilities, assigned individuals with contact information (Section 2.5) Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure (Appendix L) Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented (Section 3.5) The System Manager and ISSO review the GDIT Cloud Contingency Plan by reading the document and noting any inconsistencies or errors. When all errors are corrected, they each approve the document by signature and date. The signatures are added to the Plan Approvals page of the GDIT Cloud Contingency Plan. |
| Part b | The System Manager maintains the Contingency Plan on the secure GDIT Cloud SharePoint site where it is managed as part of the documentation baseline for the GDIT Cloud IaaS. The Contingency Plan is distributed to key personnel in two ways: Link to the GDIT Cloud SharePoint site distributed through emails to people on the Key Personnel list Hard copies made available through request and delivered via company internal mail to individuals Changes to the documentation are managed through the change management process. As changes occur to the CP, emails are sent to the key personnel to announce the change and to provide a link for online access to the Plan. The GDIT Cloud Contingency Plan identifies key personnel (Appendix A) to which copies (and updates) of the plan are distributed, including FedRAMP personnel. The CP is provided as part of the security authorization package and is made available to the JAB, FedRAMP ISSO, and GDIT Cloud teams. The key personnel contact list is maintained in Appendix A of the CP: Contingency Plan Director Alternate Contingency Plan Director Contingency Plan Coordinator Alternate Contingency Plan Coordinator Outage and Damage Assessment Lead Alternate Outage and Damage Assessment Lead Procurement and Logistics Coordinator Alternate Procurement and Logistics Coordinator Customer Communication Lead Alternate Customer Communication Lead |
| Part c | The GDIT Cloud Contingency Coordinator coordinates activities with incident response activities through careful and regular notification across the teams, along with joint meetings. In addition IR reporting is part of the annual contingency plan testing. Meetings are scheduled every six months as a forum for CP personnel and IR personnel to discuss scenarios where an incident could lead to a CP event. For example, during the course of a response to an incident, the security team may state that the Cloud needs to swap operations to the other site, thus invoking the Contingency Plan. An example of this might be if malware has infected all the Westminster machines, Cloud would swap control to Manassas using the Contingency Plan and pull all the machines in Westminster offline to resolve. These periodic meetings also allow the two teams to coordinate exercises and testing to make sure that these activities do not cause a disruption. The teams also plan IR exercises that escalate into a CP condition. Finally, CP and IR exercise and test events are preceded by notifications to all affected parties, so that no one will think the exercise is a real situation. |
| Part d | The System Manager and ISSO review the GDIT Cloud Contingency Plan annually or as changes in the system occur and updated as necessary: The annual reviews are initiated by the GDIT Cloud Security Calendar as well as embedded into Cherwell as a documentation review task. On an annual basis, the Knowledge Manager assigns a reviewer and places the KA in their review queue in the tool. The reviewer reads through the document and identifies any errors or inconsistencies with current practice or team membership. The reviewer makes updates to resolve the wording and updates the Document Revision History. All change to the policy and procedures is then reviewed by the Knowledge Manager. The results of the review are recorded both in the policy and/or procedures change page and in the Cherwell ticket. |
| Part e | The GDIT Cloud CP is updated as needed to address changes to the organization, information system, or environment of operation; and problems encountered during contingency plan implementation, execution, or testing CP-2(a)6 is the initial review and approval of the plan by someone with authority and CP-2(d) is the periodic review of the plan. CP-2(e) gets the update done for any reason. The ISSO submits a ticket, then the document is updated by the ISSO and System Manager or other roles involved in the specific update and then is approved. Updates are required in order to ensure changes are reflected in the document, to include the following: Organization changes: additions or removals of personnel or roles Environment of operation changes: removal or additional of components or capabilities Problems encountered during contingency plan implementation, execution, or testing: CP-4 requires that the contingency plan be tested periodically. Any lessons learned from the testing are integrated into document updates. Additionally, lessons learned or discovered discrepancies resulting from contingency plan implementation or execution are captured in future iterations of the document to ensure they are properly addressed. |
| Part f | The GDIT Cloud Contingency Coordinator distributes the Contingency Plan to the team (in Appendix A) when changes are made. The updated document is uploaded to the internal GDIT SharePoint site and a link is sent out to the team members as stated above. |
| Part g | The System Manager protects the Contingency Plan from unauthorized disclosure and modification by maintaining it in the Cherwell repository. All changes are governed by the change management process. Cherwell is an access controlled ticketing system which allows for document maintenance. Access is granten in accordance with procedures established for AC-2. |

### CP-3 Contingency Training (L) (M) (H)

The organization provides contingency training to information system users consistent with assigned roles and responsibilities:

1. Within [FedRAMP Assignment: ten (10) days] of assuming a contingency role or responsibility;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| CP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CP-3(a): 10 days | |
| Parameter CP-3(c): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-3 What is the solution and how is it implemented? |
| --- |
| The System Manager provides contingency training to GDIT Cloud users consistent with assigned roles and responsibilities within 10 days of assuming a contingency role or responsibility, according to GDIT Cloud IT Contingency Plan, Appendix J. The ISSO also validates that CP training has been completed before approving the update to the Contingency Plan, Appendix A Key Personnel and Team Members Contact List. Training is directed towards those who will be executing the ITCP. It usually is done with a focus on individual components, activities, and personnel associated with the plan. It’s meant to ensure that personnel who have roles in implementing the ITCP can perform their roles effectively. Computer-based training, in-house training under the guidance of security officers, and training provided by academic institutions and commercial vendors are all effective means of training those associated with this plan. At a minimum, every individual named in this plan will receive training within 10 days of assuming a contigency role or responsibility, and annually thereafter. |

### CP-4 Contingency Plan Testing (L)

The organization:

1. Tests the contingency plan for the information system [FedRAMP Assignment: at least every three (3) years] using [FedRAMP Assignment: classroom exercises/table top written tests] to determine the effectiveness of the plan and the organizational readiness to execute the plan;

CP-4(a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the JAB/AO prior to initiating testing.

1. Reviews the contingency plan test results; and
2. Initiates corrective actions, if needed.

| CP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Contingency Plan Director | |
| Parameter CP-4(a)-1: Annually for moderate impact systems | |
| Parameter CP-4(a)-2: Functional exercises for moderate impact systems | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Contingency Plan Director tests the contingency plan for the information system at least annually using functional exercises to determine the effectiveness of the plan and the organizational readiness to execute the plan. The annual test consists of an example below: The Contingency Plan Director develops test plans in accordance with NIST Special Publication 800-34 (as amended) and provides plans to FedRAMP prior to initiating testing. Test plans are approved and accepted by the Authorizing Official prior to initiating testing. After testing is completed, an AAR is conducted and the results, based on the testing and other feedback, influence the updates made to the contingency plan (this is also part (c) of this control). Testing helps to determine: The effectiveness of the plan: As the team follows the plan during testing, issues arise in executing specific plan steps, identifying areas of the plan needing improvement. Organizational readiness: Areas identified as a failure provide insight into opportunities for improvement. Failures in key areas of a test can indicate a “non-ready” state. |
| Part b | After each test, the Contingency Planning Director reviews the contingency plan test After Action Report (AAR), as an in the example below. The Contingency Plan Director then signs the report. |
| Part c | The Contingency Planning Director initiates corrective actions for areas that need adjustments and/or improvements. Adjustments can affect both the CP document and the test plans. To initiate corrective actions, the Contingency Plan Director opens Cherwell ticket(s) as appropriate to correct any deficiencies. Issues that cannot be resolved immediately are assigned to the ISSO to include in the POA&M process. |

### CP-9 Information System Backup (L) (M) (H)

The organization:

CP-9 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine what elements of the cloud environment require the Information System Backup control. The service provider shall determine how Information System Backup is going to be verified and appropriate periodicity of the check.

1. Conducts backups of user-level information contained in the information system [FedRAMP Assignment: daily incremental; weekly full]

CP-9 (a) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of user-level information (at least one of which is available online).

1. Conducts backups of system-level information contained in the information system [FedRAMP Assignment: daily incremental; weekly full];

CP-9 (b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of system-level information (at least one of which is available online).

1. Conducts backups of information system documentation including security-related documentation [FedRAMP Assignment: daily incremental; weekly full ]; and

CP-9 (c) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online).

1. Protects the confidentiality, integrity, and availability of backup information at storage locations.

| CP-9 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CP-9(a): daily incremental; weekly full and the service provider maintains at least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB. | |
| Parameter CP-9(b): daily incremental; weekly full and the service provider maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB. | |
| Parameter CP-9(c): daily incremental; weekly full and the service provider maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative. The backup storage capability is approved and accepted by the JAB | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | User-level information is not backed up separately from system-level information. See below. There are no desktop/laptops within the Infrastructure that require backup. User-level information within the Infrastructure includes data on the shared drive of the file server, and user files on the jump servers and tools. The entire file server, jump servers, and tool servers are backed up according to Part b below. |
| Part b | The System Manager conducts backups of system-level information contained in the information system daily incremental; weekly full and maintains at least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative, as follows: The GDIT Cloud encrypts replication traffic between the nodes using IPSEC and a 256-bit AES Cipher. The GDIT Cloud MMS West (primary) databases are backed up to the GDIT Cloud East storage node. The GDIT Cloud Backup Service leverages a technology that effectively takes a (synthetic) full back up every day. There is no concept of “Full” and “Incremental backups”. The GDIT Cloud Backup Service does not use tapes; it is a disk-based system. It is based on NETAPP’s SNAP Manager technology with one “Node” of backup storage in GDIT Cloud East and another “Node” in the GDIT Cloud West. The GDIT Cloud encrypts replication traffic between the Nodes using IPSEC and a 256-bit AES Cipher. The Operational procedures for the GDIT Cloud Backup Service are documented in the GDIT Cloud SharePoint Site. The Backup Service is physically inaccessible, as well as logically protected to ensure the confidentiality and integrity of the data. By default, the IaaS AlienVault backup policy and retention is to have three potential recovery points: 2 snaps per day for 12 days + 8 weeks = 32 backup copies For Customer data, the backup policy and retention is configured at customer direction/requirements. By default, the backup policy for customers is the one listed in the bullet above. The backup storage capability is approved and accepted by the JAB. |
| Part c | The System Manager conducts backups of information system documentation including security-related documentation daily incremental; weekly full and maintains at least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative, as follows: The GDIT Cloud SharePoint site - backed up as follows: (Incremental – Daily– 30 days, Weekly Full– 30 days, Yearly Full – 1 year (onsite) The GDIT Cloud Cherwell system – conforms to system backup procedure explained in Part b. The backup storage capability is approved and accepted by the JAB |
| Part d | The GDIT Cloud protects the confidentiality, integrity, and availability of backup information at storage locations by determining that all elements of the Cloud environment require the Information System Backup control. There is no tiered approach to backup. The entire system is backed up. |

### CP-10 Information System Recovery and Reconstitution (L) (M) (H)

The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

| CP-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Contingency Plan Director | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| CP-10 What is the solution and how is it implemented? |
| --- |
| The Contingency Plan Director provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure by executing the contingency plan, as described in the GDIT Cloud IT Contingency Plan, using a three-phased approach. The approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions. In general, the contingency process potentially entails three formal phases that require strict adherence to policy and procedure: 1) activation and notification, 2) recovery, and 3) reconstitution. Note: The criterion for CP is primary site (Westminster data center) is inoperable if it cannot be recovered within four (4) hours. Phase 1: Activation and Notification – Activation of the ITCP occurs after a disruption, outage, or disaster that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, loss of equipment, or other damage that typically results in long-term loss. Before the ITCP is formally activated a teleconference call is held between key personnel. The meeting provides an opportunity to resolve any issues such as key member not being able to perform their role and minor adjustments to the plan to better fit the exact situation. Once the ITCP is activated, the information system stakeholders, including customers and FedRAMP POC, are notified of a possible long-term outage, and a thorough outage assessment is performed for the affected node. Information from the outage assessment is analyzed and may be used to modify recovery procedures specific to the cause of the outage. Phase 2: Recovery – The Recovery phase details the activities and procedures for recovery of the affected system. This phase includes notification and awareness escalation procedures for communication of recovery status to system stakeholders. Phase 3: Reconstitution – The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating data and operational functionality followed by deactivation of the plan. During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational upon successful completion of validation testing. Deactivation includes activities to notify users and stakeholders of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events. |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
2. Reviews and updates the current:
   1. Identification and authentication policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Identification and authentication procedures [FedRAMP Assignment: at least annually].

| IA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter IA-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter IA-1(a): at least every 3 years | |
| Parameter IA-1(b)(1): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.7. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, identification and authentication controls in the GDIT Cloud’s GDIT-OC-PRO-IA, Identification and Authentication Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### IA-2 User Identification and Authentication (L) (M) (H)

The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

| IA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 What is the solution and how is it implemented? |
| --- |
| User Identification The GDIT Cloud uniquely identifies and authenticates organizational users by using a unique naming convention per account type, as follows: Systems acting on behalf of users are service accounts that are for application service management (e.g., SQL, Traverse, Ivanti, etc.). These accounts are also used to start/stop MS services for applications that require service accounts. Generally they have elevated privileges, thus passwords are controlled within Password Manager Pro. Note: All Portal customers will be assigned a non-privileged account. User Authentication Users are required to authenticate to the system using the following methods: Passwords: See the description for IA-5(1) in this document for details. RSA Tokens: See the description for IA-2(2), IA-2(3), IA-2(8), IA-2(11), and IA-5(11) in this document for details. |

#### IA-2 (1) Control Enhancement (L) (M) (H)

The information system implements multifactor authentication for network access to privileged accounts.

| IA-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (1) What is the solution and how is it implemented? |
| --- |
| Network Administrators implement multifactor authentication for network access to privileged accounts. All privileged access to the GDIT Cloud via network or remote access requires multi-factor authentication to access the network. This includes remote access to the GDIT Cloud via IPSEC VPN and local access from GDIT Cloud MMS Clients. In all cases, multi-factor authentication is achieved using RSA SecurID user ID and a user-defined PIN + token-defined code. GDIT Cloud users are uniquely identified by access control policy and procedure specified in the AC control family. For Network access via VPN, RSA SecurID tokens are issued for all GDIT Cloud Operations personnel per documented procedures as an integrated step in relevant GDIT Cloud personnel policies. RSA SecurID tokens are issued for GDIT Cloud Operations personnel in response to the creation of a ticket where that ticket is created and approved by the System Manager. The user ID is sent to the user separately from the shipping of the token itself. The tokens are distributed in a state where they are unusable until the recipient accesses an online location and enters his or her user ID and token code to be permitted to configure the PIN. Then, all systems comprising the GDIT Cloud leverage the RSA SecureID and/or MS Active Directory to provide GDIT Cloud MMS Authentication and Authorization services to those systems comprising the GDIT Cloud IaaS. Customer Responsibility It is responsibility of the customer to determine if they require multi-factor authentication and upon which accounts in the customer environments. GDIT Cloud provides mechanisms available to the customer if appropriate to their environment. |

#### IA-2 (12) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

IA-2 (12) Additional FedRAMP Requirements and Guidance:

Guidance: Include Common Access Card (CAC), i.e., the DoD technical implementation of PIV/FIPS 201/HSPD-12.

| IA-2 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Engineering Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-2 (12) What is the solution and how is it implemented? |
| --- |
| The Engineering Manager has configured the GDIT Cloud to accept and electronically verify Personal Identity Verification (PIV) credentials, through its FIPS 201-compliant supplier implementation, as follows: The PIV implementation is an overlay to the current Active Directory services. PIV users are uniquely identified and authenticated through the PIV authentication appliance. The PIV appliance vendor interfaces with the Federal bridge to verify the PIV card or the certificate chain has not been revoked. Customer Responsibility It is responsibility of the customer to provide and manage PIV cards according to FIPS 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors (August, 2013). The GDIT Cloud provides the mechanism to verify PIV credentials only, but does not supply or manage the PIV cards themselves. |

### IA-4 Identifier Management (L) (M)

The organization manages information system identifiers for users and devices by:

1. Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, or device identifier;
2. Selecting an identifier that identifies an individual, group, role, or device;
3. Assigning the identifier to the intended individual, group, role, or device;
4. Preventing reuse of identifiers for [FedRAMP Assignment: at least two (2) years]; and
5. Disabling the identifier after [FedRAMP Assignment: ninety days for user identifiers (see additional requirements and guidance)]

IA-4e Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period of inactivity for device identifiers.

Guidance: For DoD clouds, see DoD cloud website for specific DoD requirements that go above and beyond FedRAMP http://iase.disa.mil/cloud\_security/Pages/index.aspx.

| IA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter IA-4(a): Account Manager | |
| Parameter IA-4(d): Two Years | |
| Parameter IA-4(e): Sixty days for user and device identifiers inactivity | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud System Manager has defined and assigned account managers for the GDIT Cloud system account management as follows: SOC Manager: Authorizes accounts for SOC team members NOC Manager: Authorizes accounts for NOC team members Engineering Manager: Authorizes accounts for Infrastructure These managers provide authorization for account identifiers through creation or approval of requests in the Cherwell system. The AD administrator processes the requests and assigns the appropriate account identifier. Group Identifiers Group identifiers are not used in GDIT Cloud IaaS. Device Identifiers Device identifiers are assigned in accordance with the change management process. Engineers for each component receive authorization from an approved RFC to assign a device identifier. |
| Part b | The Account Managers manage GDIT Cloud identifiers for users and devices by selecting an identifier that identifies an individual, group, role, or device, as follows: Device Identifier Device identifiers are selected by the appropriate Engineer in accordance with the following: The GDIT Cloud utilizes an asset management process that ensures every physical device has a unique “Asset Tag” applied during the receiving process. There is also a unique hostname assigned during the logical build process. Leveraging a process that includes aspects of the devices location, operating system, platform, ownership and a 3-digit counter, the GDIT Cloud has a naming convention for devices that make sure every device ID is unique. Below is an example of how an asset identifier (server name) looks and its function: User Identifiers The GDIT Cloud users are assigned unique User IDs in the on-boarding process as defined in the GDIT Cloud Employee On-Boarding and Off-Boarding. Service Accounts Identifiers for service accounts are selected as follows: s-<functional description> Example: s-sqleng (service account for the SQL engine) |
| Part c | The Account Managers manage GDIT Cloud identifiers for users and devices by assigning the identifier to the intended individual, group, role, or device, as follows: Device Identifier Device identifiers are assigned during the logical build process for physical devices by the assigned engineer configuring the device The technology ensures that each hostname is unique, as follows: GDIT Cloud uses vCenter, which automatically checks and prohibits use of a duplicate server name. User Identifier System Administrators create and assign the user identifier during the GDIT Cloud on-boarding process where requests are made for appropriate levels access according to the GDIT Cloud Employee On-Boarding and Off-Boarding. The identifier is assigned in the system by adding the selected username to Active Directory. For non-AD integrated devices, the identifier is assigned by adding the username directly to the device. If there is a case where there is potential for two users to have the same identifier (e.g., Randy Smith and Robert Smith), additional uniqueness is added to the username that is the most recent. For example, if Randy Smith (rsmith) were already a user at the time that Robert Smith onboarded, Robert Smith would be assigned the username “rsmith2”. |
| Part d | The Account Managers manage GDIT Cloud identifiers for users and devices Preventing reuse of user identifiers for at least two years, as follows: Devices Device names are selected and assigned by the implementer/integrator. The implementer will then submit a task to the Configuration Manager (CM), following KA 11638 for hardware, for the name(s) to be recorded in the CMDB. The CM will verify if there is an existing CI with the same hostname prior to adding the CI. This prevents device names from being re-used for the life of the system. If a device name is inserted into the CMDB that matches a previously selected device name, it will be listed as a duplicate name. In this case the Configuration-Change Manager alerts the assigned Engineer via email. The device name is updated to ensure non-duplication for the life of the hostname. Requests for Change may replace an existing device with an upgraded device using the same hostname. For VMs, the implementer will select and assign a hostname and the cloud automation tool will verify that the current vCenter environment does not contain an existing hostname prior to deploying a new VM. This will prevent duplicate hostnames from existing in vCenter. The cloud automation tool will then create a new CI entry into the CMDB for the newly deployed VM.Users The Account Managers prevent reuse of identifiers for users for at least two years. All account identifiers are retained in disabled status for at least two years after end of use. When a new account is needed, the software refuses to allow a duplicate. The Account Manager adds additional complexity to the new user’s identifier as described in part c of this control prior to assigning an identifier. |
| Part e | The Account Managers manage GDIT Cloud identifiers for users by disabling the identifier after sixty days for user identifiers and 60 days for device inactivity, as follows: The System Administrator configures Active Directory to automatically run a script that facilitates disabling user identifiers (accounts) after 60 days of inactivity. The script runs daily and produces a report showing accounts that have been inactive for 60 days or more. If any accounts are found, a Cherwell ticket is generated and the Account Manager reviews it to have those accounts disabled. Non-AD integrated appliances and devices are configured by the specific engineer to automatically disable user accounts after 60 days of inactivity. Device identifiers (host names, IP addresses) are not automatically disabled. Host names and IP addresses are tracked as part of the CMDB tracking process. As devices are decommissioned, the device identifiers are disabled. |

### IA-5 Authenticator Management (L) (M)

The organization manages information system authenticators by:

1. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;
2. Establishing initial authenticator content for authenticators defined by the organization;
3. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
4. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
5. Changing default content of authenticators prior to information system installation;
6. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
7. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type].
8. Protecting authenticator content from unauthorized disclosure and modification;
9. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and
10. Changing authenticators for group/role accounts when membership to those accounts changes.

**IA-5 Additional FedRAMP Requirements and Guidance:**

**Requirement:** Authenticators must be compliant with NIST SP 800-63-3 Digital Identity Guidelines IAL, AAL, FAL level 1. Link <https://pages.nist.gov/800-63-3>.

| IA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-5(g): 60 days for passwords | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager manages information system authenticators by verifying, as part of the initial authenticator (RSA SecureID) distribution, the identity of the individual, group, role, or device receiving the authenticator, as follows: Individual Authenticators For individual authenticators, there are two components involved in authentication: 1) password; and 2) RSA SecurID token. The RSA token and PIN are used to remotely access the jumpserver. Once the user accesses the jumpserver, they may access other resources by either using their Active Directory password (Windows and RHEL servers) or by using their password for non-AD integrated devices. Distributing Initial User Authenticators: Passwords GDIT Cloud users are provided with a GDIT corporate email account through which corporate and other communications are conducted. Prior to onboarding with GDIT, each employee’s identity is positively verified by the GDIT Human Resources department by examining the employee’s government issued identification (e.g., driver license, state ID, military ID, passport, etc.). After positive identity is established, the employee is issued a GDIT corporate email account with the following address format: firstname.lastname@gdit.com . Example: john.cavitt@gdit.com. Because of the identity verification process and the consistent email address format, GDIT Cloud Account Managers have a reasonable process by which to verify a user’s identity in order to distribute initial account authenticators. When an account is set up in GDIT Cloud (Active Directory and any non-AD integrated devices as applicable), the Account Manager sends the initial authenticator content (initial password) to the user via their GDIT corporate email account. Distributing Initial User Authenticators: RSA Tokens GDIT Cloud users are issued RSA SecurID tokens that are either hardware tokens or soft tokens. Hard tokens are either distributed directly to the user in person by the Account Manager or are mailed to a physical address that the user provides to the Account Manager through their GDIT corporate email account. The Account Manager sends the hardware token viaFedEx, or other delivery service provider. Token PINs are set up by the user upon first login. Tokens are distributed in a state where they are unusable until the user activates it by entering his or her user ID and token code to be permitted to configure the PIN. The PIN is a six digit code chosen by the user. Instructions to receive a soft token are emailed to the user via their corporate email address. The user downloads an RSA token application to their mobile device and must activate it using the information in the email. Group/Role Authenticators GDIT Cloud does not use group or role authenticators. Device Authenticators Device authenticators as defined by NIST SP 800-53 IA-5 supplemental guidance include certificates and passwords. Cloud Engineers and System Administrators are able to establish the identity of devices by using the device’s hostname and/or the device’s IP address. Devices use root passwords as authenticators. Access to root password for systems is defined in GDIT Cloud Policy on Root Password Access. Effectively, the one-time passwords are stored in the Password Manager Pro system. Access to the passwords will be permitted by role based access to the system owners. Any use of the accounts must be documented with a ticket containing the system name, and reason for needing the root password. Once the password has been retrieved from the Password Manager and used, a new password must be generated. Root passwords must meet complexity and length requirements and per GDIT Cloud process but be generated by an approved tool in the GDIT Cloud MMS Suite of tools and updated within the Password Manager. |
| Part b | The System Manager manages information system authenticators by establishing initial authenticator content for authenticators, as follows: Individual Authenticators Initial account passwords are generated by the System Administrator in accordance with complexity rules described for IA-5(1). The password is sent to the user through email with no other identifying information. The tokens are distributed in a state where they are unusable until the recipient enters his or her user ID and token code to be permitted to configure the PIN. RSA’s SecurID binds user IDs to Token serial numbers. To initialize a Token, the user accesses the GDIT Cloud VPN where he or she is prompted to enter the userID and the current code displayed on their token. If the code entered matches the expected code known by the RSA server for that token, the user is required to create a unique PIN code. If not, the attempt to authenticate is refused. Once that first authentication is successful, subsequent authentication requests must include the user ID, PIN, and token code. Device Authenticators When a system has a root password configured, it is configured at installation time . The password complexity for root passwords is 14 characters long with at least one character meeting each of the following: upper case letters, lower case letters, numbers, and special characters. The password is stored in Password Manager Pro which enforces access control and the password complexity requirements. |
| Part c | The System Manager manages information system authenticators by ensuring that authenticators have sufficient strength of mechanism for their intended use, as follows: RSA is configured to require certain lengths of authenticators and also apply complexity requirements to user PIN codes. Token codes are 6 digits and change every 60 seconds. PIN codes are 8 digits. In conjunction with passwords, RSA token codes provide adequate strength of mechanisms for remote access to GDIT Cloud. The RSA SecureID appliance does not accept PINs that do not meet the appropriate criteria. GDIT Cloud administered Linux-based systems and Microsoft-based systems are all configured to apply complexity requirements to user passwords via GPO settings as required by STIG Vuln ID #V-1150. This setting ensures that AD integrated accounts (which are required to access the jumpserver and subsequently, the Cloud environment) meet the password complexity requirements cited as part of IA-5(1) and are, therefore, of sufficient strength of mechanism for the environment. Root Passwords must meet complexity and length requirements cited as part of IA-5(1) and must be generated by Password Manager Pro in the GDIT Cloud MMS suite of tools. |
| Part d | The System Manager manages information system authenticators by establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; Initial Authenticator Distribution For individual authenticators, there are two components involved in authentication: 1) password; and 2) RSA SecurID token. The RSA token and PIN are used to remotely access the jumpserver. Once the user accesses the jumpserver, they may access other resources by either using their Active Directory password (Windows and RHEL servers) or by using their password for non-AD integrated devices. Distributing Initial User Authenticators: Passwords GDIT Cloud users are provided with a GDIT corporate email account through which corporate and other communications are conducted. Prior to onboarding with GDIT, each employee’s identity is positively verified by the GDIT Human Resources department by examining the employee’s government issued identification (e.g., driver license, state ID, military ID, passport, etc.). After positive identity is established, the employee is issued a GDIT corporate email account with the following address format: firstname.lastname@gdit.com . Example: john.cavitt@gdit.com. Because of the identity verification process and the consistent email address format, GDIT Cloud Account Managers have a reasonable process by which to verify a user’s identity in order to distribute initial account authenticators. When an account is set up in GDIT Cloud (Active Directory and any non-AD integrated devices as applicable), the Account Manager sends the initial authenticator content (initial password) to the user via their GDIT corporate email account. Distributing Initial User Authenticators: RSA Tokens GDIT Cloud users are issued RSA SecurID tokens that are either hardware tokens or soft tokens. Hard tokens are either distributed directly to the user in person by the Account Manager or are mailed to a physical address that the user provides to the Account Manager through their GDIT corporate email account. The Account Manager sends the hardware token via FedEx, or other delivery service provider. Token PINs are set up by the user upon first login. Tokens are distributed in a state where they are unusable until the user activates it by entering his or her user ID and token code to be permitted to configure the PIN. The PIN is an eight digit code chosen by the user. Instructions to receive a soft token are emailed to the user via their corporate email address. The user downloads an RSA token application to their mobile device and must activate it using the information in the email. Lost/Compromised or Damaged Authenticators Passwords In the event a password becomes compromised, the user whose password became compromised must report the fact to the GDIT Cloud service desk, generating a Cherwell incident. At any time the user may change his/her password unless the account has been locked out. If the account is locked out, the System Administrator unlocks the account, resets the password ensuring that the “change password on next login” box is checked. The System Administrator transmits the new temporary password to the user by sending an unmarked email to the user’s known GDIT corporate email address. The user can log back into the system and must change their password upon login. RSA Tokens In the event a token becomes lost/compromised or damaged, the user must report the fact to the Cloud service desk. The System Administrator creates a Cherwell incident and assigns the incident ticket to the Network Operations Center to immediately disable the token in the RSA appliance. The user is then issued a new token according to the process outlined in the steps above. This process is the same for hard and soft tokens. Revoking Authenticators Authenticators are revoked in the following cases: A temporary or emergency account was established for maintenance or other purposes and is no longer needed. In this case, the Engineer working with the vendor creates a Cherwell incident ticket to have the account and its authenticator revoked. The account/authenticator is revoked in accordance with procedures outlined for AC-2. A user is terminated from the system. Procedures outlined for AC-2 are followed in this case. |
| Part e | The System Manager manages information system authenticators by changing default content of authenticators prior to information system installation, as follows: Since RSA SecurID tokens (both hardware and software tokens) are time driven, there is no default content to replace. As part of the GDIT Cloud build process, all other hardware “as shipped default” authenticators have been changed. This includes the RSA SecurID application and network devices. The Engineer responsible for the respective system ensures the appropriate hardening guidelines are followed and that default authenticators are changed. |
| Part f | The System Manager manages information system authenticators by establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators, as follows: RSA Tokens and PINs RSA Token PINs remain the same and, therefore, do not have a maximum lifetime; however, given the function of the tokens, each authentication credential has an enforced maximum lifetime restriction of 60 seconds. There is not a minimum lifetime restriction set for RSA tokens codes and PINs. Active Directory Account Authenticators Minimum and Maximum Lifetime Restrictions The Windows Engineer has configured (as implemented for IA-5(1) part d) the Active Directory authenticators through the use of GPO settings as follows: Minimum lifetime restrictions 1 day Maximum lifetime restrictions 60 days Conditions for Authenticator Reuse The Windows Engineer has configured (as implemented for IA-5(1) part e) the Active Directory authenticators through the use of GPO settings as follows:Reuse conditions Passwords may not be reused for 24 generations |
| Part g | The System Manager manages information system authenticators by establishing a process to ensure that authenticators are changed/refreshed every 60 days for passwords. RSA Tokens and PINS RSA Token PINs remain the same and, therefore, are not refreshed; however, given the function of the tokens, each authentication credential has an enforced refresh rate of 60 seconds. Active Directory Account Authenticators Access to Windows, RHEL and Active Directory authenticated applications and services requires initial login using a valid MS Active Directory username and password. All MS Active Directory account passwords must be changed/refreshed every 60 days. This is enforced by GPO settings configured by the Windows Engineer. Password authentication is an additional step following multi-factor authentication through RSA. |
| Part h | The System Manager manages information system authenticators by protecting authenticator content from unauthorized disclosure and modification, as follows: Individual Responsibilities (PL-4, PS-6) GDIT Cloud Operations team members are instructed never to release their PIN or password to anyone, per GDIT Cloud general acceptable use policy and GDIT Cloud Rules of Behavior . Protection of Authenticators at Rest Windows and RHEL OS protect authenticators stored within the servers by using a one-way hash. If the password files were to be compromised, the plaintext passwords would not be viewable. The Windows Engineer has configured the Windows server in accordance with STIG Vuln ID #V-2372 (Disable reversible password encryption). The Linux engineer has configured RHEL servers not to store passwords in the /etc/passwd file. All password hashes must be stored in the /etc/shadow file using the SHA512 hash (STIG vulnerability ID #’s V-38499, V38574, RHEL-07-010170, RHEL-07-010180). Protection of Authenticators in Transit The Network Engineer has configured the VPN to encrypt all traffic in transit and thus includes PINs, tokens, and passwords, through the use of IPSec. |
| Part i | The System Manager manages information system authenticators by requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators, as follows: The GDIT Cloud Operations team members never release their PIN and account passwords to anyone, per GDIT Cloud general acceptable use policy and GDIT Cloud Rules of Behavior . “You must maintain the confidentiality of your authentication credentials such as your password. Do not reveal your authentication credentials to anyone; a General Dynamics IT employee should never ask you to reveal them.” Devices are configured to do hashing functions and encryption as described in part h above. |
| Part j | The System Manager manages information system authenticators by changing authenticators for group/role accounts when membership to those accounts changes, as follows: Engineers are responsible for the appropriate system accounts appropriate to their subject matter. When an engineer changes responsibility, the newly assigned engineer changes the password through Password Manager Pro to ensure the authenticators are changed as required |

#### IA-5 (1) Control Enhancement (L) (M)

The information system, for password-based authentication:

1. Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];
2. Enforces at least the following number of changed characters when new passwords are created: [FedRAMP Assignment: at least one (1)];
3. Stores and transmits only cryptographically-protected passwords;
4. Enforces password minimum and maximum lifetime restrictions of [Assignment: organization- defined numbers for lifetime minimum, lifetime maximum];
5. Prohibits password reuse for [FedRAMP Assignment: twenty-four (24)] generations; and
6. Allows the use of a temporary password for system logons with an immediate change to a permanent password.

**IA-5 (1) a and d Additional FedRAMP Requirements and Guidance:**

**Guidance:** If password policies are compliant with NIST SP 800-63B Memorized Secret (Section 5.1.1) Guidance, the control may be considered compliant.

| IA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter IA-5(1)(a): case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters and Mobile devices are excluded from the password complexity requirement | |
| Parameter IA-5(1)(b): at least one or as determined by the information system (where possible) | |
| Parameter IA-5(1)(d): one day minimum, sixty day maximum | |
| Parameter IA-5(1)(e): twenty four | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | System Administrators configure the GDIT Cloud information system for password-based authentication to leverage the Active Directory ID and password authentication to enforce a minimum password complexity to be case sensitive, minimum of twelve characters, and at least one each of upper-case letters, lower-case letters, numbers, and special characters, as follows: VPN Access GDIT Cloud VPN solution utilizes multi-factor authentication for VPN access to the environment to access all systems hosts, including Windows and RHEL. Cloud solution administrators are required to use a 6 character PIN in addition to their RSA SecurID token which is commensurate with their increased levels of access, which equals a total authenticator length of 12 characters. Host Access (Servers, Network Devices, Appliances) System host access requires an additional Active directory ID and Password. The configured password complexity parameters are as follows: Minimum number of characters: 14 Complexity requirements at least one upper case character; at least one lower case character; at least one number; and at least one special character. User access to servers (RHEL, Windows, VMware) and databases are governed by the Active Directory user ID password and all associated requirements as enforced by the GPOs set by System Administrators in the domain controllers. Network devices are governed by TACACS+ user ID password which coordinates with Active Directory for the authentication and thus inherits the Active Directory controls for password complexity. Appliances and root passwords are required by policy, as stated in control IA-5 part b, to match the Active Directory password complexity rules. |
| Part b | System Administrators configure the GDIT Cloud to leverage the Active Directory ID to enforce at least the following number of changed characters when new passwords are created: at least 1. The minimum number character change is enforced by GPOs which are configured by System Administrators. User access to servers (RHEL, Windows, VMware) and databases are governed by the Active Directory user ID password and all associated requirements as enforced by the GPOs set by System Administrators in the domain controllers. Network devices are governed by TACACS+ user ID password which coordinates with Active Directory for the authentication and thus inherits the Active Directory controls for password change requirements. Appliances and root passwords are required by policy, as stated in control IA-5 part b, to match the Active Directory password change configuration. |
| Part c | System Administrators configure the GDIT Cloud network access to leverage the Active Directory ID to store and transmit only cryptographically-protected passwords, as follows: Protection of Authenticators at Rest Windows and RHEL OS protect authenticators stored within the servers by using a one-way hash. If the password files were to be compromised, the plaintext passwords would not be viewable. The Windows Engineer has configured the Windows server in accordance with STIG Vuln ID #V-2372 (Disable reversible password encryption). The Linux engineer has configured RHEL servers not to store passwords in the /etc/passwd file. All password hashes must be stored in the /etc/shadow file using the SHA512 hash (STIG vulnerability ID #’s V-38499, V38574, RHEL-07-010170, RHEL-07-010180). Protection of Authenticators in Transit The Network Engineer has configured the VPN to encrypt all traffic in transit and thus includes PINs, tokens, and passwords, through the use of IPSec. See SC-8 for additional detail. User access to servers (RHEL and Windows), network devices, databases, and appliances are governed by the Active Directory user ID/password and all associated requirements as enforced by the GPOs set by System Administrators in the domain controllers. |
| Part d | System Administrators configure the GDIT Cloud network access to leverage the Active Directory ID to enforce password minimum and maximum lifetime restrictions of one day minimum, sixty day maximum, as follows: Minimum lifetime restriction: 1 day Maximum lifetime restriction: 60 days User access to servers (RHEL, Windows, VMware) and databases are governed by the Active Directory user ID password and all associated requirements as enforced by the GPOs set by System Administrators in the domain controllers. Network devices are governed by TACACS+ user ID password which coordinates with Active Directory for the authentication and thus inherits the Active Directory controls for password change requirements. Appliances and root passwords are required by policy, as stated in control IA-5 part b, to match the Active Directory password change configuration. |
| Part e | System Administrators configure the GDIT Cloud network access to leverage the Active Directory ID to prohibit password reuse as follows: The GDIT Cloud prohibits password reuse for 24 generations as set in Active Directory. User access to servers (RHEL, Windows, VMware) and databases are governed by the Active Directory user ID password and all associated requirements as enforced by the GPOs set by System Administrators in the domain controllers. Network devices are governed by TACACS+ user ID password which coordinates with Active Directory for the authentication and thus inherits the Active Directory controls for password history controls. Appliances and root passwords are required by policy, as stated in control IA-5 part b, to match the Active Directory password history controls. |
| Part f | System Administrators configure the GDIT Cloud network access to leverage the Active Directory ID to allow the use of a temporary password for system logons with an immediate change to a permanent password, as follows: The System Administrator, when receiving a Cherwell ticket to establish a user account as described in AC-2, sets up the account, inputs the initial temporary password and ensures that the “change password on next login” box is checked. When the user first logs in, they will be prompted to immediately change their password to a permananent one. User access to servers (RHEL, Windows, VMware) and databases are governed by the Active Directory user ID password and all associated requirements as enforced by the GPOs set by System Administrators in the domain controllers. Network devices are governed by TACACS+ user ID password which coordinates with Active Directory for the authentication and thus inherits the Active Directory controls for password change on next login requirements. Appliances and root passwords are required by policy, as stated in control IA-5 part b, to match the Active Directory password configuration. However, not all appliances have the technology to enforce this requirement. |

#### IA-5 (11) Control Enhancement (L) (M) (H)

The information system, for hardware token-based authentication, employs mechanisms that satisfy [Assignment: organization-defined token quality requirements].

| IA-5 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-5(11): separate hardware token (key fob) or soft-token application deployed on a smartphone using different seed values for each token; token codes must change on a time schedule | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-5 (11) What is the solution and how is it implemented? |
| --- |
| The System Manager, for hardware token-based authentication, employs mechanisms that satisfy token quality requirements defined by the organization as follows: GDIT Cloud has deployed RSA SecurID token-based multi-factor authentication system. Each token, whether a hardware token (key fob) or a soft token, is seeded separately through the use of a factory-encoded random key. Each token generates a 6-digit authentication code at 60 second intervals using a built-in clock and the token's factory-encoded random key The appliance, which also has a real-time clock and a database of valid tokens with the associated seed records, authenticates a user by computing what number the token is supposed to be showing at that moment in time and checking this against what the user entered. These features are not configured but are built into the system. |

### IA-6 Authenticator Feedback (L) (M) (H)

The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

| IA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-6 What is the solution and how is it implemented? |
| --- |
| All GDIT Cloud systems and MMS Clients are configured to obscure credentials during feedback (i.e., passwords are shown as asterisk \*\*) |

### IA-7 Cryptographic Module Authentication (L) (M) (H)

The information system implements mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

| IA-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-7 What is the solution and how is it implemented? |
| --- |
| All systems comprising the GDIT Cloud leverage the RSA SecureID and/or MS Active Directory. Both RSA Secure ID and MS Active Directory are certified to meet FIPS 140-2 cryptographic requirements. Customer Responsibility Customers are responsible for configuring their web browsers, mobile devices, etc., to enable communications through encryption. Customers will achieve FIPS 140-2 encryption for data transmitted. In addition, Customers are responsible for implementing the Transmission Integrity, Transmission Confidentiality, Use of Cryptography, and Session Authenticity controls for the applications that Customers establish within their Virtual Machine environments. |

### IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H)

The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

| IA-8 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 What is the solution and how is it implemented? |
| --- |
| System Administrators have configured the GDIT Cloud to uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users). Only GDIT personnel are allowed to access the GDIT Cloud FedRAMP boundary. Non-organizational users (Customers) only have access to their customer environments. With no authorization to access the GDIT Cloud IaaS. Customer Responsibility Customers are responsible to ensure that each individual or process acting on behalf of a user for both organization and non-organizational users have a unique account within their virtual machines and supported applications. The Customer is responsible for controlling access to their VM. Customers are responsible for ensuring that they designate only the required and authorized individuals for access to the GDIT Cloud. |

#### IA-8 (1) Control Enhancement (L) (M) (H)

The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies.

| IA-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (1) What is the solution and how is it implemented? |
| --- |
| System Administrators have configured the GDIT Cloud to accept and electronically verify Personal Identity Verification (PIV) credentials provided by other federal agencies through our CA-PAM implementation that is FIPS-201 complaint. See SA-4(10) and IA-2(12). System Administrators configure the CA-PAM solution to overlay AD, meaning that it does talk with AD. It creates a mapping between the PIV card and an AD account. CA-PAM solution uses the PIV card as the ‘what you have’ factor and the PIN card set for that PIV card as the ‘what you know’ factor. The CA-PAM solution intercepts authentication requests, checks if a PIV is involved and handles that authentication. If not, it passes the authentication step to RSA or AD (for user/pw). AD accounts can be set for PIV-only, or any combination of the three authentication methods. The GDIT Cloud is not configured to enforce PIV only, but can accept PIV and can configure any particular account to PIV-only. The use of PIV cards is not currently a requirement inside the GDIT Cloud IaaS. Customer Responsibility It is responsibility of the customer to provide and manage PIV cards. The GDIT Cloud provides the mechanism to verify PIV credentials only, but does not supply or manage the PIV cards themselves. |

#### IA-8 (2) Control Enhancement (L) (M) (H)

The information system accepts only FICAM-approved third-party credentials.

| IA-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (2) What is the solution and how is it implemented? |
| --- |
| The System Manager does not support or allow general public access to IaaS through public-facing websites. All users must access the GDIT Cloud through it FIPS 140-2 VPN, which requires multi-factor authentication or PIV authentication. Therefore this control is N/A since the GDIT Cloud does not trust any credentials issued by third-party, nonfederal government entities. |

#### IA-8 (3) Control Enhancement (L) (M) (H)

The organization employs only FICAM-approved information system components in [Assignment: organization-defined information systems] to accept third-party credentials.

| IA-8 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-8(3): GDIT Cloud | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (3) What is the solution and how is it implemented? |
| --- |
| The System Manager does not support or allow general public access to IaaS through public-facing websites. All users must access the GDIT Cloud through a FIPS 140-2 VPN, which requires multi-factor authentication: either RSA or PIV authentication. Therefore this control is N/A since the GDIT Cloud does not trust any credentials issued by third-party, non-federal government entities. |

#### IA-8 (4) Control Enhancement (L) (M) (H)

The information system conforms to FICAM-issued profiles.

| IA-8 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IA-8 (4) What is the solution and how is it implemented? |
| --- |
| The System Manager does not support or allow general public access to IaaS through public-facing websites. All users must access the GDIT Cloud through a FIPS 140-2 VPN, which requires multi-factor authentication; either RSA or PIV authentication. Therefore this control is N/A since the GDIT Cloud does not trust any credentials issued by third-party, non-federal government entities. |

## Incident Response (IR)

### IR-1 Incident Response Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and
2. Reviews and updates the current:
   1. Incident response policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Incident response procedures [FedRAMP Assignment: at least annually].

| IR-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter IR-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter IR-1(b)(1): at least every 3 years | |
| Parameter IR-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| IR-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.8. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, incident response controls in the GDIT Cloud’s GDIT-OC-PRO-IR, Incident Response Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### IR-2 Incident Response Training (L) (M)

The organization provides incident response training to information system users consistent with assigned roles and responsibilities in accordance with NIST SP 800-53 Rev 4:

1. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility;
2. When required by information system changes; and
3. [FedRAMP Assignment: at least annually] thereafter.

| IR-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter IR-2(a): 30 days to Incident Response Team | |
| Parameter IR-2(c): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud Security Operations Manager (SOC Manager) provides incident response training within 30 days to Incident Response Team system users consistent with assigned roles and responsibilities described in the Incident Response Plan, GDIT Cloud Incident Response Plan. Training sign-in sheets and/or Completion Certificates are saved in the secure GDIT Cloud SharePoint site (Operations Training folder) along with the training tracker spreadsheet. Training materials (brown bag slide decks) are saved in the “Training” shared folder in techservices that are accessed via the GDIT Cloud workstations. In order to become proficient with incident response and handling and build skills, SOC team members are periodically presented with a security scenario and will be observed by a senior team that will document the exercise and ask the SOC responder questions pertaining to the scenario and procedure. At the conclusion of the exercise, the observer will complete the observer’s exercise documentation, and this will include lessons-learned in regards to the applicable security procedure(s) and SOC responder’s execution. The lessons-learned may result in updates to the security procedure documentation and / or remedial training for the exercise’s SOC responder. NIST Special Publication 800-61 Rev2 (August 2012) Appendix A contains examples of security handling exercises and related questions. Although the GDIT Cloud SOC team may use a scenario documented in Appendix A, scenarios are not limited to the NIST 800-61 Rev 2 (August 2012) document. |
| Part b | The GDIT Cloud Security Operations Manager, when required by information system changes, generates/updates incident response training materials to reflect any change to the IR process. Examples of changes to the information system that could require additional or updated incident response training includes, but is not limited to the following: Addition of new hardware/software/capabilities; Removal of hardware/software/capabilities; Changes in team/personnel structure; Changes in or updates to IR processes/procedures; or Changes to the system’s risk posture, including new threats and vulnerabilities. The GDIT Cloud Security Operations Manager facilitates IR training in an ongoing and dynamic manner, meaning that training topics are updated frequently as the threat landscape changes or when a topic area is identified that needs to be covered more in depth based on testing results or other factors. The change to standard training is in the form of brown bag lunch sessions, that describe the changes introduced to the IR process. These trainings are delivered to the Engineering, NOC, and SOC personnel. |
| Part c | The SOC Manager provides GDIT Cloud Engineering, NOC, and SOC personnel annual IR refresher training that covers each phase of the IR process: Detection and analysis Containment Eradication Recovery Post-incident Training sign-in sheets and/or Completion Certificates are saved in the secure GDIT Cloud SharePoint site (Operations Training folder) along with the training tracker spreadsheet. The annual training is included on the Security Calendar that contains the continuous monitoring FedRAMP requirements. |

### IR-4 Incident Handling (L) (M) (H)

The organization:

1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
2. Coordinates incident handling activities with contingency planning activities; and
3. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

IR-4 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider ensures that individuals conducting incident handling meet personnel security requirements commensurate with the criticality/sensitivity of the information being processed, stored, and transmitted by the information system.

| IR-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Operations Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Security Operations Manager implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery, as described in the GDIT Cloud Incident Response Plan. Following the FedRAMP template, the sections include incident handling that follows the process from security incident identification through security incident closure. The Plan provides the process for incident handling that includes preparation, detection and analysis, containment, eradication, recovery, and post incident: |
| Part b | The Security Operations Manager coordinates incident handling activities with contingency planning activities. Incident response (handling) is included within the contingency plan (and testing). Incident response testing is conducted within the Contingency Plan Table Top exercise. |
| Part c | The Security Operations Manager incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. The GDIT Cloud ISSO, (in conjunction with Customer ISSO), reviews the Security Incident Report and conducts Lessons Learned exercises based on incident reports. |

### IR-5 Incident Monitoring (L) (M) (H)

The organization tracks and documents information system security incidents.

| IR-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analysts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-5 What is the solution and how is it implemented? |
| --- |
| Security Analysts track and document information system security incidents, as follows: In the event of a security incident, Security Analysts take ownership of the incident, create a Ticket in GDIT Cloud Ticketing system and notify the GDIT Cloud security team to investigate and remediate. Upon resolution, GDIT Cloud security team generates a post mortem After Action Report with root cause analysis. See GDIT Cloud Incident Response Plan ). |

### IR-6 Incident Reporting (L) (M) (H)

The organization:

1. Requires personnel to report suspected security incidents to the organizational incident response capability within [FedRAMP Assignment: US-CERT incident reporting timelines as specified in NIST SP800-61 (as amended)]; and
2. Reports security incident information to [Assignment: organization-defined authorities].

IR-6 Additional FedRAMP Requirements and Guidance

Requirement: Report security incident information according to FedRAMP Incident Communications Procedure.

| IR-6 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter IR-6(a): US-CERT incident reporting timelines as specified in NIST Special Publication 800-61, as amended | |
| Parameter IR-6(b): US government stakeholders including end-user agencies and US-CERT according to FedRAMP Incident Communications Procedure | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in The reporting requirements are dictated by the US-CERT Federal Reporting Guidelines at http://www.us-cert.gov/government-users/reporting-requirements as cited in NIST SP 800-61, August 2012, Revision 2, section 2.3.4.3. The following table outlines timelines for reporting GDIT Cloud security incidents to FedRAMP. The SOC Manager or ISSO are responsible for ensuring the report is sent to FedRAMP. The GDIT Cloud incident response procedures provide appropriate security incident documentation to FedRAMP and/or US-CERT reporting requirements. At the point in the incident response process where we have ascertained that the incident is not a false positive and have performed the appropriate triage, Security Analysts will follow the escalation process as defined for the incident type and notify the appropriate people/organizations as soon as possible. |
| Part b | The ISSO reports security incident information to US government stakeholders including end-user agencies and US-CERT according to FedRAMP Incident Communications Procedure, as described in the GDIT Cloud Incident Response Plan. The following table identifies the GDIT Cloud security procedures that are used for responding to incidents as well as reporting incidents to the applicable stakeholders. |

### IR-7 Incident Response Assistance (L) (M) (H)

The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

| IR-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Security and Network Analysts | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-7 What is the solution and how is it implemented? |
| --- |
| Customer users can contact the GDIT Cloud Service Desk on a Toll Free number that will be provided at the time of contract signature. GDIT Cloud Analysts will create a ticket in the help desk system to track communication with the Customer user. GDIT Cloud Analysts will update GDIT managers with updates on a scheduled basis, in accordance with established SLA’s. GDIT Cloud’s Information Security Team provides 24 x 7 support for all suspected GDIT Cloud system security incidents. All requests for assistance are documented in the GDIT Cloud MMS Ticketing system (which includes automated notification and escalation), reviewed by information security team, and responded to, based on priority. The GDIT Cloud MMS SIEM receives syslog streams from all devices that are monitored in the GDIT Cloud. The GDIT Cloud SIEM leverages syslog correlation capabilities to generate alerts regarding security, performance, and system activity anomalies. |

### IR-8 Incident Response Plan (L) (M) (H)

The organization:

1. Develops an incident response plan that:
   1. Provides the organization with a roadmap for implementing its incident response capability;
   2. Describes the structure and organization of the incident response capability;
   3. Provides a high-level approach for how the incident response capability fits into the overall organization;
   4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
   5. Defines reportable incidents;
   6. Provides metrics for measuring the incident response capability within the organization;
   7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   8. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
2. Distributes copies of the incident response plan to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance].

IR-8(b) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Reviews the incident response plan [FedRAMP Assignment: at least annually];
2. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing;
3. Communicates incident response plan changes to [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance].

IR-8(e) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel.

1. Protects the incident response plan from unauthorized disclosure and modification.

| IR-8 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter IR-8(a)(8):System Manager, SOC Manager, ISSO | |
| Parameter IR-8(b): Computer Security Incident Response Team (CSIRT) and management as defined in Section 2.3 in the IRP | |
| Parameter IR-8(c): at least annually | |
| Parameter IR-8(e): IRP team and management as defined in Section 2.3 in the IRP | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| IR-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | (1) The Operations Manager developed an incident response plan that provides the organization with a roadmap for implementing its incident response capability. All functions performed by the DCIRT are primarily and fundamentally in line with the six-step FISMA theoretical model which encompasses Prevention, Detection, Containment, Eradication, Recovery, and Follow-up. The GDIT Cloud Incident Response Plan contains the following items: Introduction GDIT Cloud Policies and Procedures Training Security Exercises Incident Management Overview The Resources and Management Support Organizational Structure Critical Security Incident Response Team Contact List Roles and Responsibilities Structure and Organization of the Incident Response Capability Roadmap for implementing the GDIT Cloud incident response capability Incident Response Capability for the GDIT Cloud Incident Response Capability for the Customer GDIT Cloud Tools Incident Reporting and Tracking Tools System Monitoring Tools Security Incident Response – High-Level Process Workflow Incident Response Handling Incident Response Reporting Incident Tracking Incident Response Assistance External Information Sources Internal Information Resources Incident Response Metrics Plan Testing GDIT Cloud Incident Response (IR) Plan Review APPENDIX A: Customer Point of Contact Information APPENDIX B: Vendor Point of Contact Information (2) The IR Plan describes the structure and organization of the incident response capability. The GDIT Cloud leverages the processes in GDIT Cloud Policy on Security Incident Response to guide our team’s response to incidents irrespective of client. This incident response policy provides GDIT Cloud with a roadmap for implementing its incident response capability and describes the structure and organization of the incident response capability. Within the GDIT Cloud Operations organizational structure, the SOC Analysts provide monitoring and analysis for network traffic and endpoint events. Once an incident is identified, it is identified as one of six categories in (See Table 4.1). The category of the incident is directly related to the risk it poses to the Data Center environment and operational mission. At this point, the GDIT Cloud SOC performs incident response activities. A risk assessment is performed for each incident that includes determining the incident’s characteristics (e.g. target system(s) involved, source of incident, type of incident) as compared to the incident’s severity, which is a composite function of the potential customer business impact of the incident and the level of exposure. Once the determination has been made of the incident’s origin, a custom signature will be developed for deployment throughout the GDIT Cloud infrastructure to prevent reoccurrence. Using this repeatable lifecycle approach to GDIT Cloud incidents will keep the Data Center on the leading edge of security. After each incident, the SOC will conduct a lessons learned meeting to review events from ongoing incident handling activities and to incorporate the resulting changes into incident response procedures, training, and testing/exercises. Proven and repeatable processes will ensure that the GDIT Cloud infrastructure continues to be protected against new and evolving threats. The OCIRT follows GDIT SEC-PRO-IT-73.1 INCIDENT RESPONSE process and adopted comprehensive process, based on industry best practices to manage an incident throughout its lifecycle. This process is based on the six-step NIST theoretical model that encompasses Preparation, Detection and Analysis, Containment, Eradication, Recovery and Post-Incident Activities. Security incidents are tracked via ticketing software in Cherwell. Security Incident Response procedures guide SOC (Security Operations Center) personnel through the security incident response process. (3) The IR Plan provides a high-level approach for how the incident response capability fits into the overall organization, as follows: GDIT Cloud Operations follows the GDIT Cloud Incident Response Plan process to manage an incident throughout its lifecycle. This process is based on the 6-step FISMA theoretical model which encompasses Prevention, Detection, Containment, Eradication, Recovery, and Follow-up. Proven and repeatable processes will ensure that the Data Center infrastructure continues to be protected against new and evolving threats. Within the GDIT Cloud Operations organizational structure, the SOC Analysts provide monitoring and analysis for network traffic and endpoint events. Once an incident is identified, it is prioritized into one of six categories listed in GDIT Cloud Incident Response Plan. The category of the incident is directly related to the risk it poses to the Cloud environment and operational mission. At this point, the GDIT Cloud Incident Response Team (DCIRT) performs incident response activities. A risk assessment is performed for each incident that includes determining the incident’s characteristics (e.g. target system(s) involved, source of incident, type of incident) as compared to the incident’s severity, which is a composite function of the potential Customer business impact of the incident and the level of exposure. Once the determination has been made of the incident’s origin, a custom signature will be developed for deployment throughout the GDIT Cloud IaaS to prevent reoccurrence. Security incidents are tracked by the GDIT Cloud MMS Ticketing system. Security Incident templates guide DCIRT personnel through the security incident response process as defined in the GDIT Cloud Incident Response Plan . After each incident, the DCIRT will conduct a Lessons Learned meeting to review events from ongoing incident handling activities and incorporate into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. (4) The IR Plan meets the unique requirements of the organization, which relate to mission, size, structure, and functions. The DCIRT reports suspected security incidents to the HCSD organization elements responsible for incident response capability within organization-defined time periods listed in the GDIT Cloud Incident Response Plan. Customer system-specific Incident Response reporting time periods will be established during the Customer On-boarding process. At the top is GDIT IT Security. GDIT IT Security coordinates security incidents internally and externally. Below is the division level HCSD Security. HCSD Security provides information to HCSD management and GDIT IT Security on all security incidents. At the root of the organizational structure is GDIT Cloud Operations. The GDIT Cloud Incident Response Team (DCIRT) performs Incident response activities in accordance with GDIT Cloud policy, applicable standards, and program requirements. The DCIRT reports Incidents to HCSD Security who reports to the JAB. (5) The IR Plan defines reportable Incidents as listed in the Table below. (6) The IR Plan provides metrics for measuring the incident response capability within the organization as follows: IR-1 Notification of Critical Infrastructure Faults 100% notifications within one hour Using email and GDIT Cloud MMS Ticketing system IR-2 Security Event Detection 90% detected within 30 minutes Using GDIT Cloud MMS Ticketing system to document the anomaly IR-3 Security Event Analysis to determine risk of potential anomaly 90% Initiated within 30 minutes from detection Using GDIT Cloud MMS Ticketing system to document the initial analysis IR-4 Quarantine of Suspect System if security incident is determined 95% completed within 60 minutes Using GDIT Cloud MMS Ticketing system, Documented coordinated actions taken to quarantine of validated compromise IR-5 Security Event Analysis Status Reporting 95 % within 1 hour after determination of a security incident Using email and GDIT Cloud MMS Ticketing system, provide a status update to GDIT Security Management IR-6 Security Anomaly Investigation Report as a final analysis 90% within 10 days Using Word template for documentation of a validated security incident attached to GDIT Cloud MMS Incident Ticket (7) The IR Plan defines the resources and management support needed to effectively maintain and mature an incident response capability. GDIT management supports the GDIT Cloud as a core business goal. Its support for an effective and efficient incident response capability is clearly in line with this goal. To respond quickly to potential incidents requires both automation and personnel. GDIT management has procured the technology to automate GDIT Cloud’s Incident Response capability and has provided the GDIT Cloud SOC personnel to implement this incident response plan. (8) This IR Plan is reviewed and approved for implementation by the following designated organizational officials: System Manager and the ISSO. |
| Part b | The Security Operations Manager securely distributes copies of Incident Response Plan (IR Plan) to the Incident Response Team identified in Section 2.3 of the GDIT Cloud Incident Response Plan . The IR Plan is distributed securely via Cherwell (through the KA) and through the internal SharePoint site. The JAB is included in the distribution via upload to MAX.gov. The Security Operations Manager defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. |
| Part c | The Security Operations Manager reviews the GDIT Incident Response Plan annually: The annual reviews are initiated by the GDIT Cloud Security Calendar as well as embedded into Cherwell as a documentation review task. On an annual basis, the Knowledge Manager assigns a reviewer and places the KA in their review queue in the tool. The reviewer reads through the document and identifies any errors or inconsistencies with current practice or team membership. The reviewer makes updates to resolve the wording and updates the Document Revision History. All changes to the document are then reviewed by the Knowledge Manager. The results of the review are recorded both in the document change page and in the Cherwell ticket. |
| Part d | The Security Operations Manager updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing. These changes are then communicated to the individuals that form the Incident Response Team as part of the annual IR Training. The GDIT Cloud Incident Response Plan is updated as needed to address changes to the organization, information system, or environment of operation; and problems encountered during incident response. The Security Operations Manager submits a ticket, then the document is updated by the ISSO and System Manager or other roles involved in the specific update and then is approved. Updates are required in order to ensure changes are reflected in the document, to include the following: Organization changes: additions or removals of personnel or roles Environment of operation changes: removal or additional of components or capabilities System/organizational changes or problems encountered during plan implementation, execution, or testing |
| Part e | The Security Operations Manager communicates incident response plan changes to the Incident Response team identified in Section 2.4 of the IR Plan, when changes are required. The IR Plan is maintained in Cherwell, which tracks the updates and approvals of any changes. In addition, any change to the IR Plan requires CMB approval and the approvals are documented in change management board minutes. The GDIT Cloud defines a list of incident response personnel (identified by name and/or by role) and organizational elements. The incident response list includes designated FedRAMP personnel. |
| Part f | The Security Operations Manager protects the incident response plan from unauthorized disclosure and modification by ensuring that it is maintained on the secure GDIT Cloud SharePoint site, which is internal to GDIT and is access controlled. |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system maintenance policy and associated system maintenance controls; and
2. Reviews and updates the current:
   1. System maintenance policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System maintenance procedures [FedRAMP Assignment: at least annually].

| MA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MA-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter MA-1(b)(1): at least every 3 years | |
| Parameter MA-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.9. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, system maintenance policy and associated controls in the GDIT Cloud’s GDIT-OC-PRO-MA, System Maintenance Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### MA-2 Controlled Maintenance (L) (M) (H)

The organization:

1. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
2. Approves and monitors all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
3. Requires that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;
4. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs;
5. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
6. Includes [Assignment: organization-defined maintenance-related information] in organizational maintenance records.

| MA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MA-2(c): System Manager | |
| Parameter MA-2(f): ; Date and time of maintenance; Name of the Company; Name of individual(s) performing the maintenance; Name of escort, if applicable; Description of maintenance performed; List of equipment removed or replaced (including identification numbers, if applicable) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT maintains a maintenance contract with all hardware vendors and software providers. Access to the data center area is limited to GDIT Cloud employees and approved vendor personnel. Vendor maintenance personnel are escorted as necessary by GDIT Cloud staff to the appropriate area where the maintenance work is to be performed. The objective of the maintenance program is to preserve the physical integrity of the equipment by adhering to recommended maintenance schedules and operating conditions. System administrators differentiate between hardware and software maintenance. Hardware maintenance is performed under a maintenance contract or warranty Software maintenance is performed by a team of programmers in most cases Many customer-impacting systems in the GDIT Cloud cannot be taken off-line to perform unscheduled maintenance. System administrators schedule maintenance (both hardware and software) for GDIT Cloud systems to limit down time and maximize their services to the customer base. System administrators perform all routine maintenance on servers and supporting infrastructure in accordance with GDIT Cloud software and hardware vendor best practices. Maintenance logs are maintained (in the form of service or change requests tracked in the GDIT Cloud MMS Ticketing system) for all system components, which include the following: Date and time of maintenance Name of the Company Name of individual(s) performing the maintenance Name of escort, if applicable Description of maintenance performed List of equipment removed or replaced (including identification numbers, if applicable) |
| Part b | System administrators directly approve and monitor all maintenance activities of the GDIT Cloud IaaS. Maintenance activities can be performed on-site or remotely depending on the nature of the maintenance activity which would dictate whether the equipment is serviced on-site or removed to another location. All maintenance is scheduled leveraging the CR process. This ensures that maintenance is done at approved times, proper procedures are followed, and all appropriate stack holders are informed. Each site maintains logs of physical maintenance that is performed on site. These records include: Date and time of maintenance Name of person performing maintenance Description of maintenance being performed List of equipment/tools being brought into the site Sign off of escort who verified the tools/equipment for malware Maintenance performed on the virtual infrastructure follows the procedures captured in KA 10595, SOP: GDIT Cloud Patching. If a manufacturer, vendor, or developer-provided maintenance schedule does not exist, the system must be reviewed annually to determine if maintenance is required. IT technical support and maintenance work performed at GDIT Cloud facilities (on-site) must be supervised by or under the control of GDIT Cloud personnel knowledgeable in appropriate IT operations. Any systems that are taken off-site for maintenance or repair are inventoried and tracked. Maintenance logs are also maintained by the vendors under their contractual maintenance agreement. |
| Part c | No equipment is permitted to be taken off site for repairs. GDIT maintains service contracts for all physical equipment that includes onsite replacement and/or repair. Equipment is only removed from the site after it has been decommissioned and disposal procedures have been completed. The System Manager and/or system owner shall approve the removal of any information system components from the facility when maintenance or repairs are necessary. |
| Part d | All physical devices have associated disposal procedures. These procedures include media sanitization equipment, techniques, and procedures documented in the GDIT-OC-PRO-MP-1.0, Media Protection Procedures). |
| Part e | During maintenance affecting security application upgrades or servicing security hardware, enhancements, or replacements, the GDIT Cloud Security Analysts and System Administrators team together to perform operational checks to ensure potentially impacted security controls are still functioning properly following maintenance or repair actions. |
| Part f | The maintenance record contains the following: Date and time of maintenance Name of the Company Name of individual(s) performing the maintenance Name of escort, if applicable Description of maintenance performed List of equipment removed or replaced (including identification numbers, if applicable in organizational maintenance records. |

### MA-4 Remote Maintenance (L) (M) (H)

The organization:

1. Approves and monitors nonlocal maintenance and diagnostic activities;
2. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;
3. Employs strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;
4. Maintains records for nonlocal maintenance and diagnostic activities; and
5. Terminates session and network connections when nonlocal maintenance is completed.

| MA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT Cloud approves and monitors all nonlocal maintenance. Maintenance is performed over the network after login to the jump hosts as the approved method. Network connections to the devices require access and authentication to the jump hosts before the network is available. All maintenance activities are tracked and approved through a change request process governed by the CAB. The implementation of the change is tracked in the GDIT Cloud MMS Ticketing system. All maintenance is performed during predefined maintenance windows. |
| Part b | The use of non-local maintenance and diagnostic tools is only performed by authorized System Administrators. The GDIT Cloud does not allow 3rd party, non-local maintenance and diagnostic testing without prior review by a System Administrator that is documented in a service ticket. |
| Part c | Access to all GDIT Cloud Information systems requires multi-factor authentication. During a remote maintenance session the local system administrator logs into the jump host. The GDIT Cloud administrators logically connect to each host and perform activities locally through IPSEC sessions. Prior to gaining access to the environment, administrators must be connected to GDIT Cloud’s internal network. The user accesses the data center network through an encrypted VPN connection. A unique user ID is used as the identifier and a SecurID token passcode combined with a PIN is used as the authenticator. |
| Part d | GDIT Cloud records all maintenance, remote or local, in a CR. This ensures records are uniform and are approved by all appropriate stakeholders. Maintenance records are stored in Cherwell, the ticket management system. |
| Part e | Non-local maintenance is performed through IPSEC sessions. GDIT Cloud staff manually terminates the session after the maintenance is completed. |

### MA-5 Maintenance Personnel (L) (M) (H)

The organization:

1. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel;
2. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and
3. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

| MA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT Cloud System Manager will only grant access to authorized maintenance personnel in accordance with the GDIT Cloud Identification and Authentication Procedure. |
| Part b | The GDIT Cloud FSO maintains the following for anyone who has access authorization: GDIT Cloud Roster Authorized Vendors list Authorized Vendor Personnel list |
| Part c | The only unescorted personnel allowed to perform maintenance, (i.e., patch VMs through Ivanti) are GDIT Cloud employees who go through the employee on-boarding process. This process ensures that appropriate background checks, security training, approvals, etc. are completed before an employee is given an Active Directory account and associated token. Only users that are in the NOC/SOC Active Directory group are able to log into Ivanti. When maintenance personnel do not have the necessary access authorizations, GDIT Cloud Staff with the appropriate access authorizations will escort and supervise maintenance personnel AT ALL TIMES during the performance of maintenance activities on the information system in accordance with the GDIT Cloud Physical and Personnel procedures. Maintenance personnel without the necessary access authorizations will never be without an escort while in a GDIT Cloud secure area. |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
2. Reviews and updates the current:
3. Media protection policy [FedRAMP Assignment: at least every three (3) years]; and
4. Media protection procedures [FedRAMP Assignment: at least annually].

| MP-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MP-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter MP-1(b)(1): at least every 3 years | |
| Parameter MP-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| MP-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.9. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, system media protection policy and associated controls in the GDIT Cloud’s GDIT-OC-PRO-MP-1.0, Media Protection Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### MP-2 Media Access (L) (M)

The organization restricts access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].

| MP-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MP-2-1: ; Paper; External hard drives | |
| Parameter MP-2-2: defined personnel | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-2 What is the solution and how is it implemented? |
| --- |
| The SOC Manager restricts access to the following types of media: Paper Break Glass account password (onpaper) Domain Administrator account password (breakglass) Cisco breakglass account password External Hard Drives Iron Key external drive (FIPS 140-2 encrypted) Aegis Padlock DT external hard drive Access is restricted access as follows: Paper Break Glass (paper) = Authorized individuals are only permitted access as defined in the Roles and Privileges Matrix. KA 10815 Emergency Breakglass Account Procedure describes the process to store, manage, and retrieve the breakglass account passwords. Authorized individuals are listed in KA 10667 (described below) by name. External Hard Drives Authorized personnel are permitted access to the drives as described in KA 10667, Approved Media Transport Personnel, which describes, by name, who is authorized to access and transport the media (drives and paper). KA 10668 Approved Removable Media SOP and Inventory, describes the process of obtaining removable media from secure storage. |

### MP-6 Media Sanitization and Disposal (L) (M)

The organization:

1. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and
2. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

| MP-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter MP-6(a)-1: External Portable Drives | |
| Parameter MP-6(a)-2: GDIT Cloud sanitization techniques and procedures | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | System Administrators sanitize external media prior to disposal, release out of organizational control, or release for reuse using media sanitization equipment, techniques, and procedures documented in the GDIT-OC-PRO-MP-1.0, Media Protection Procedures that contains the following information: 4.2 Media Access 4.3 Media Labeling 4.4 Media Storage 4.5 Media Transport 4.6 Media Sanitization and Disposal 4.7 Media UseThe procedures are further supplemented with the following SOPs: KA 10992 Cloud Media Sanitization Procedure describes the procedure that GDIT Cloud uses for sanitization of media. KA10723 - How To: Handling Requirements for External Portable Drives KA10666 - GDIT Cloud Chain of Custody Form Since the GDIT Cloud is a Moderate security categorization, GDIT Cloud personnel implement the media sanitization decision path recommended in section 4.0 (p. 17) of NIST 800-88, Guidelines for Media Sanitization. GDIT Cloud uses the decision path for the moderate security categorization. |
| Part b | The GDIT Cloudemploys sanitization mechanisms withstrengthand integritycommensurate with the classification orsensitivityof the information and approved by the ISSO. The GDIT Cloud uses the following tools for media sanitization: BC Wipe: Software tool used to overwrite hard disk media in accordance with 5220.22-M. This tool writes a series of ones with a verification, followed by a serios of zeros with a verification, followed by random data with a verification. Applied Magnetics Laboratory AMC-6KG Degaussing Wand: GSA approved tool used to sanitize hard disk drives or any other magnetic media if they cannot be wiped using BC Wipe. To degauss disk storage devices, wipe the degaussing wand onto each side of the disk platter so that the active magnetic portion of the degaussing wand completely covers the recording surface of the disk from hub to perimeter. Wipe at least three times always maintaining physical contact between the degaussing wand and the disk platter. If disks are part of a sealed hard disk drive assembly, they must be removed for degaussing. Erasure of hard disk drives causes damage that prohibits their continued use. |

### MP-7 Media Use (L) (M) (H)

The organization [Selection: restricts; prohibits] the use of [Assignment: organization-defined types of information system media] on [Assignment: organization-defined information systems or system components] using [Assignment: organization-defined security safeguards].

| MP-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter MP-7-1: prohibits | |
| Parameter MP-7-2: all system external media except:; Iron Key devices; Aegis Padlock DT | |
| Parameter MP-7-3: GDIT Cloud IaaS system components | |
| Parameter MP-7-4: Tripwire | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| MP-7 What is the solution and how is it implemented? |
| --- |
| The System Manager prohibits the use of all external media on all Cloud IaaS system components via Group Policy which disables the use of removable storage media. External storage media is defined as the Iron Key devices and the Aegis Padlock DT listed in the GDIT Cloud removable media inventory (KA10668 Approved Removable Media Checkout and Inventory). Approved, encrypted external hard drives are controlled by the SOC. The Iron Key and Aegis Padlock DT external/removable hard drives (FIPS 140-2 encryption) are the only removable digital media allowed in the GDIT Cloud If the approved removable media need to be used in the GDIT Cloud system, the Group Policy prohibiting such activity must be disabled temporarily in accordance with KA 10693 Request USB Storage Exemption. |

## Physical and Environmental Protection (PE)

### PE-1 Physical and Environmental Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and
2. Reviews and updates the current:
   1. Physical and environmental protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Physical and environmental protection procedures [FedRAMP Assignment: at least annually].

| PE-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PE-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter PE-1(b)(1): at least every 3 years | |
| Parameter PE-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PE-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s physical environment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.9. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, system physical environment policy and associated controls in the GDIT Cloud’s GDIT-OC-PRO-PE, System Physical Environment Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### PE-2 Physical Access Authorizations (L) (M)

The organization:

1. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;
2. Issues authorization credentials for facility access;
3. Reviews the access list detailing authorized facility access by individuals [FedRAMP Assignment: at least annually]; and
4. Removes individuals from the facility access list when access is no longer required.

| PE-2 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-2(c): Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The FSO develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides, including vendors, according to the Physical And Environmental Protection Standard Operations Procedure: Access to both facilities’ Cloud assets is controlled by access lists developed and maintained by the FSO. The list is approved by the site FSO. The list is maintained through the use of quarterly reviews. Access to the GDIT Cloud facility is segregated based on the duties of each individual. The facility containing the data center in Westminster has physical access controls for the office area, the NOC and SOC area, and the data center. Personnel are granted badge access to those areas depending on their assigned duties. Access authorizations are reviewed at least quarterly by the Facility Security Officer (FSO). Security logs of scanned badges are kept and generated reports are made by the Program Security Officer and are given to the FSO to show admittance and rejection for every badge reader in the building. GDIT Cloud East This facility does not contain offices and is minimally staffed by COPT security personnel. COPT provides reporting and auditing of all access to the site and client areas. Badge access lists are supplied monthly to GDIT: GDIT HCSD- cardholders Report – provides the list of authorized individuals to the main GDIT floor GDIT HCSD cardholders – cage in a cage – provides the list of authorized individuals to the inner cage. GDIT - Cage in a Cage Cardholder Report– provides the Cardholder list for Cage Access The FSO authorizes or removes personnel from the list by contacting COPT and making the request. The access list is reviewed annually as part of the SOC3 audit process COPT completes. GDIT performs this annually or as the personnel change. |
| Part b | The FSO issues authorization credentials for facility access according to Physical And Environmental Protection Standard Operations Procedure, Version 1.3 (5/26/16): The process for conducting monthly reviews is as follows: Request access lists for both GDIT Cloud East and GDIT Cloud West facilities. Upon receipt, review each list to determine if: all personnel on the list are current employees; all personnel on the list are required to have access based on their job duties; and there are any personnel not on the list that need to be on the list. After review, if there are any personnel listed that need removed from access for any reason, the FSO emails the appropriate point of contact to request removal: GDIT corporate for GDIT Cloud West and COPT for GDIT Cloud East. For personnel identified as needing access but not on the list, the FSO requests access in the same manner as was done for access removal. See step 3 above. |
| Part c | The FSO and ISSO review the access list monthly and the ISSO reviews annually as part of continuous monitoring. GDIT Cloud East Reports are sent monthly to the Cloud East FSO. GDIT - Cardholder Report –contains the Cardholder List by company are reviewed monthly by the East Coast Security Operations Manager (Acting as the FSO) The list of people are compared against the list of GDIT employed personnel (Email Verifications). Exceptions to the analysis are deemed "incorrect authorizations" and are removed from the list. GDIT HCSD - Cage 203E –contains the Cage Access History Report |
| Part d | According to Physical And Environmental Protection Standard Operations Procedure, the FSO and ISSO reviews the access list monthly and removes individuals from the facility access list when access is no longer required. GDIT Cloud West When an employee terminates for any reason, GDIT HR department contacts the corporate security department to ensure all badge access is removed. This process ensures that if the employee’s badge is not collected upon leaving the facility, the employee would not be able to access any GDIT facility to include the GDIT Cloud West facility. GDIT Cloud East In the event of a termination or when an employee no longer needs access to the GDIT Cloud East data center, the FSO contacts COPT and requests that the person’s name be removed from the badge access list. |

### PE-3 Physical Access Control (L) (M) (H)

The organization:

1. Enforces physical access authorizations at [Assignment: organization-defined entry/exit points to the facility where the information system resides] by:
   1. Verifying individual access authorizations before granting access to the facility; and
   2. Controlling ingress/egress to the facility using [FedRAMP Assignment: CSP defined physical access control systems/devices AND guards];
2. Maintains physical access audit logs for [Assignment: organization-defined entry/exit points];
3. Provides [Assignment: organization-defined security safeguards] to control access to areas within the facility officially designated as publicly accessible;
4. Escorts visitors and monitors visitor activity [FedRAMP Assignment: in all circumstances within restricted access area where the information system resides];
5. Secures keys, combinations, and other physical access devices;
6. Inventories [Assignment: organization-defined physical access devices] every [FedRAMP Assignment: at least annually]; and
7. Changes combinations and keys [FedRAMP Assignment: at least annually] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.

| PE-3 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-3(a): All physical access points | |
| Parameter PE-3(a)(2): Physical control systems and guards | |
| Parameter PE-3(b): All physical access points | |
| Parameter PE-3(c): security safeguards | |
| Parameter PE-3(d): in all circumstances within restricted access area where the information system resides | |
| Parameter PE-3(f)-1: physical access device annually | |
| Parameter PE-3(f)-2:annually | |
| Parameter PE-3(g): The FSO enforces physical access authorizations at defined entry/exit points to the facility where the information system resides by verifying individual access authorizations before granting access to the facility; and controlling ingress/egress to the facility using physical access control systems/devices and guards. GDIT Cloud West Verifying Individual Access Authorizations Prior to requesting access for an employee or contractor, the FSO verifies the individual is authorized to access the physical area for which they are requesting access. Once the access is verified, the FSO sends a request to GDIT corporate to have the employee’s badge added to the access list for the specific area. Controlling Ingress/Egress to the Facility The defined entry/exit points to the facilities and how ingress/egress is controlled for each follows: Access to the GDIT Cloud West data center is through doors 2, 4, and 5. Door 2 (Primary data center access) Requires proximity card access Access is monitored through badge activity CCTV monitored Door 3 (Data center emergency exit only) Access from the outside has been disabled (door handle removed and replaced with a plate) Door is locked from the inside Door is sensored, alarmed, and CCTV monitored Door 4 (UPS room) Requires proximity card access Access is monitored through badge activity CCTV monitored Door 5 (UPS room exterior door) Mechanical door lock Sensored and CCTV monitored The data center administrative, Service Desk, NOC, and SOC areas are also controlled by an electronic access system that is maintained by GDIT Headquarters in Virginia. There are proximity card readers and locks to the building’s perimeter that are on a separate access control system, and it is maintained by a commercial real estate management service. The building’s perimeter doors are unlocked during each business day from 6 AM to 8 PM and are programmed to lock automatically off-hours and weekends. These doors are also monitored by the same commercial real estate management service. The GDIT Cloud Operations Center is occupied by GDIT Employees performing the role of Technical Support. This area is restricted to GDIT personnel and vendors who are authorized to work in this area, or have a valid business reason to be in this area. The data center floor houses the hardware used to provide services to customers. This area is restricted to GDIT personnel and vendors who are authorized to work in this area. The Communications closet and PBX room house voice and network communication equipment. These areas are restricted to GDIT personnel and vendors who are authorized to work in these areas. GDIT Cloud East Verifying Individual Access Authorizations Prior to requesting access for an employee or contractor, the FSO verifies the individual is authorized to access the physical area for which they are requesting access. Once the access is verified, the FSO sends a request to COPT to have a badge created and added to the access list for the specific area. Controlling Ingress/Egress to the Facility The facility has four areas that control ingress/egress to the East facility: Entrance to the data center compound. This regulates access to the outside of the data center building including the parking area. This is monitored and controlled by security guard staff 24x7. Entrance to the building. This is monitored and controlled by security guard staff 24x7. Entrance to the data center. Access to this area requires badge access and biometrics. Entrance to the GDIT data center cage. Access to this area requires badge access and biometrics. The GDIT Cloud East resides in a secure facility that includes: vehicle arrest barriers, K12 rated perimeter fencing, guarded entrances, multiple recorded video surveillance zones, facility access control via a badge access card access system, biometric authentication for GDIT suites, man traps, continuous monitoring, and 24x7 on premise security personnel and staffing. All exit doors are alarmed. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Physical access audit logs are maintained for the following entry/exit points : GDIT Cloud West GDIT corporate maintains the physical access audit logs for the Cloud West facility as part of their physical security controls. The following entry/exit points generate audit logs that are maintained by GDIT corporate: Data center administrative area Two badge access doors Data center SOC/NOC area Two badge access doors Door #2 (Primary data center access) Door #4 (UPS room) On a monthly basis, GDIT corporate sends the FSO badge access activity reports (audit logs) for review that show which badges were used to access which area and when (date/time). GDIT Cloud East COPT maintains the physical access audit logs for badge accesses to the data center area and to the GDIT cage inside the data center. On a monthly basis, COPT sends the FSO the badge access activity report (audit logs) for review that shows badge activity for the GDIT cage and Cage in a Cage inside the data center. |
| Part b | The FSO provides security safeguards to control access to areas officially designated as publicly accessible, as appropriate, in accordance with the system’s assessment of risk. GDIT Cloud West Access to common areas is controlled by entry from the parking lot to the front door and a log of visitors in that area is kept and sent to the ISSO monthly. The Lobby of the facility is the primary location for all individuals entering the center. All secure entry and exit points have electronic badge readers and monitoring via video camera surveillance. GDIT Cloud East The GDIT Cloud East provides a layered defense for physical security of the data center. All areas of the site require controlled access. There is no public space within 150 feet of the building. Access to the area where the GDIT Cloud data center cages reside is controlled by a proxcard and biometric authentication. All visitors are questioned and authenticated via an identity verification system. Security guard team must open the door. Access to the data center where GDIT Cloud resides (Level 3), and all ingress and egress points are controlled by a card reader (depending on physical access restrictions) and there are biometrics locks (Finger Print) on the cage doors. The card reader is controlled by a terminal in the security center that maintains logs of who has accessed, which doors, and successful and unsuccessful access attempts. Guests are on a guest list for the day, The FSO provides the list to the site security guard staff. Guests are required to provide government issued identification documentation to the guard and GDIT escort must validate before the guard will issue a visitor badge that allows them to access the main hall. The badge enables the Guest to pass though the man-trap. From there the GDIT escort will take over. |
| Part c | According to Physical And Environmental Protection Standard Operations Procedure, the FSO requires escorts for visitors and monitors visitor activity in all circumstances within restricted access area where the information system resides. The visitor is required to sign-in before being assigned an escort The visitor is assigned an escort that must be with the visitor at all times within the Cloud facility The visitor is required to sign-out when leaving the Cloud facility |
| Part d | GDIT Cloud West The FSO secures keys, combinations, and other physical access devices by use of a centrally-managed and controlled key lockbox in NOC and SOC and secure combinations by placing them in locked containers. GDIT Cloud East COPT manages and ensures that the following physical access devices are secure at the East facility: Badge readers Biometric finger scanners |
| Part e | GDIT Cloud West The FSO conducts an annual inventory of badge readers, and keys at the West facility. GDIT Cloud East COPT conducts a monthly inventory of badge readers and biometric scanners. |
| Part f | GDIT Cloud West The FSO changes combinations and keys when access keys are lost or combinations are compromised, as follows: Access to the GDIT Cloud West assets is managed solely by badge access control devices. There are no keys used to access the GDIT Cloud components. See the process of physical access written in PE-3. GDIT Cloud uses a combination safe to store authorized media (see MP-4 for details). The Facilities Manager ensures that the combination is changed on an annual basis or in the event that the combination is compromised, or individuals are transferred or terminated. GDIT Cloud East Access to the GDIT Cloud East assets is managed solely by badge and biometric access control devices. There are no keys or combinations used to access the GDIT Cloud components. See the process of physical access written in PE-3. |
| Part g | Click or tap here to enter text. |

### PE-6 Monitoring Physical Access (L) (M) (H)

The organization:

1. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents;
2. Reviews physical access logs [FedRAMP Assignment: at least monthly] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
3. Coordinates results of reviews and investigations with the organization’s incident response capability.

| PE-6 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-6(b)-1: monthly | |
| Parameter PE-6(b)-2: organization-defined events or potential indications of events | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT Cloud West The FSO and NOC personnel monitor physical access to the facility where the information system resides to detect and respond to physical security incidents. The FSO reviews physical access logs for the areas described in PE-3 to determine if any anomalous activities occurred. Examples of anomalous activities include but are not limited to: 1) access during non-business hours to areas typically not accessed during those times; 2) access by personnel who do not typically access an area (though they may have been granted access); and/or 3) multiple failed access attempts (failed badge swipes) to an area at any time. If the activity cannot be associated with known/approved maintenance activities, the FSO follows up with the employee’s supervisor to determine the cause of the anomaly. Through CCTV cameras set up as described in PE-3, the FSO can also review footage of the date/time the anomalous activity was detected. Additionally, monitors showing the live feed of the various CCTV cameras are set up on the NOC area, allowing NOC personnel to view activity in those areas 24x7. The surveillance cameras provide continuous coverage of the data center entry/exit points and automatically commence recording when motion is detected. If an incident is detected through another means (e.g., SIEM solution), if needed, the FSO can view footage of the specific area concerned based on the date/time stamp. This enhances the incident response capability for physical as well as logical security incidents, if needed. GDIT Cloud East Cameras and access control systems are monitored 24x7 by the COPT Security Guards. |
| Part b | The GDIT Cloud ISSO reviews physical access logs on a monthly basis for the areas described in PE-3 to determine if any anomalous activities occurred. Examples of anomalous activities include but are not limited to: 1) access during non-business hours to areas typically not accessed during those times; 2) access by personnel who do not typically access an area (though they may have been granted access); and/or 3) unauthorized access indicated by surveillance of an area at any time. If the activity cannot be associated with known/approved maintenance activities, the ISSO follows up with the employee’s supervisor to determine the cause of the anomaly. In the event the cause is unapproved, open an incident ticket. The incident ticket process is consistent with processes described in the IR family of controls, specifically IR-4 Incident Handling within this document. GDIT Cloud West The ISSO also reviews physical access logs in the event of a suspected physical access incident or other event. Examples of these potential indications of events include but are not limited to: Maintenance and/or visitor logs are not completed or are inconsistent; Hardware is reported missing and there is no ticketing record for its removal; Hardware is out of place (e.g., rack doors opened for unknown reason); or A door alarm is tripped. Additionally, any of the above events can be further investigated by reviewing the CCTV recorded events according to date/time stamp. GDIT Cloud East COPT provides physical access logs to the FSO on a monthly basis. The logs provided are as follows: GDIT HCSD - Cage 203E - history of access to the GDIT floor GDIT HCSD – Cage in a cage – history of access to the inner cage GDIT HCSD Visitor log - history of escorted visitors COPT provides 24x7 on-site monitoring of the East facility to include the data center room and the cage in which GDIT Cloud assets are deployed. GDIT Cloud SOC personnel contact COPT security personnel in the event that anomalous system activity is observed on or related to Manassas deployed assets. In this case COPT reviews their access logs to determine if there was an associated physical access of the GDIT Cloud East cage at that time. |
| Part c | GDIT Cloud West The GDIT Cloud ISSO coordinates results of reviews and investigations with the incident response capability team: The individuals fulfilling the roles above are documented in the IR Plan referenced below. The CSIRT reviews the information provided by the FSO and follows the GDIT Cloud Incident Response Plan section 3.4. GDIT Cloud EAST The GDIT Cloud ISSO reviews physical access logs on a monthly basis provided by COPT as described in part b of this control. Any questionable access is presented to site management and vetted with GDIT team members to provide a second source of validation. The GDIT Cloud incident response team is informed of any GDIT Cloud cage related physical access violation so they can begin an investigation as part of the IR process. |

### PE-8 Visitor Access Records (L) (M) (H)

The organization:

1. Maintains visitor access records to the facility where the information system resides for [FedRAMP Assignment: for a minimum of one (1) year]; and
2. Reviews visitor access records [FedRAMP Assignment: at least monthly]

| PE-8 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-8(a): for a minimum of one year | |
| Parameter PE-8(b): monthly | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT Cloud West The FSO collects access information from visitors to the facility where the information system resides. The ISSO receives copies of those records on a monthly basis. The ISSO records the results of the record review in the ticket in Cherwell which is maintained for at least one year. Visitors accessing the facility must provide: i) name and organization of the visitor, ii) signature of visitor, iii) form of identification, iv) date of visit, v) time of entry and departure, vi) purpose of visit, name and organization of person visited. GDIT Cloud East COPT security personnel maintain access records for visitors that includes i) name and organization of the visitor, ii) signature of visitor, iii) form of identification, iv) date of visit, v) time of entry and departure, and vi) purpose of visit. All visitors to the East facility are required to notify security one day in advance of the visit. COPT also maintains records of the notification of visit to verify a visitor once they arrive. All visitors are required to present a valid form of identification. |
| Part b | GDIT Cloud West The FSO reviews visitor access log monthly and reports the results to the ISSO. The ISSO also reviews logs Monthly as part of continuous monitoring. The ISSO records the results of the record review and any follow-up actions in a ticket in Cherwell. GDIT Cloud East (COPT provides the ISSO with monthly visitor access logs. The ISSO reviews the logs and records the results of the record review any follow-up actions in a ticket in Cherwell. |

### PE-12 Emergency Lighting (L) (M) (H)

The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

| PE-12 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-12 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud Data Center facilities maintains battery-powered emergencylighting systems that automaticallysupplies light to the GDIT Cloud Data Center areasin the event ofpowerloss to the primarypowersupply. The emergencylighting ensures that emergency exits and evacuation routes aresufficientlylighted in the event ofpowerloss in the building. The GDIT Cloud Data Center emergencylighting system is incorporated into the design ofthe facilitythat houses the GDIT Cloud Data Center. Theseunits are tested annuallyduringthe annual facilitytesting. The emergency lighting system in the GDIT Cloud Data Center is mounted onthe exit doorleadingto additional emergency exits throughout the facility. The emergencylighting unit has its own battery chargeablepack plugged into electricmains to keep it charged. The GDIT Cloud Data Center Contact Center also has emergencylightingunits installed into the ceilingin conjunction with thestandard lighting system. GDIT Cloud East: Emergency lighting is in place of a power failure and all lighting is on generator back up. |

### PE-13 Fire Protection (L) (M) (H)

The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

| PE-13 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-13 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud Data Center has automatic firesuppressors with aheat-sensor system built into the entire facilityhousingthe GDIT Cloud Data Center. In conjunction with GDIT Cloud Data Center management, Facilities Management tests the system annuallyto certify readiness in the event ofa fire. The firesuppression system in the GDIT Cloud Data Center is separate from the system used in the rest ofthebuilding. (PE-15) To ensure added protection from waterdamage, the system is adry-pipe system which uses compressed airin the lines to detect leaks. In the event ofadetection (smokeorheat), thelines are charged with water. Unlikeadeluge system, the data center’s firesuppression system onlydischarges waterthrough sprinklersthat havebeen activated through heat. Ifthereis a false positive activation, water can bemanually drained from thelines bypushinga releasebutton insidethe GDIT Cloud data center restricted areajust outsidethe DataCenter door. There aresmoke detectors mounted on the ceilingsofthedata center and the Contact Center area. Thesedetectors haveamonitoring alerts system that notifies security personnel of anysmoke alerts. Aftera fire/event notification is received bythe facility security personnel, an inspection oftheproblem area(s)is conducted for further reporting and escalation to facilitymanagement and/or emergencypersonnel. There is one hand held HalotronIModel 5HB-2 fire extinguisher of rating5 – B:C installed in thedata center. HalotronIis a clean fire extinguishing agent that quickly and effectively protects GDIT Cloud data center assets without generating an undesirablesolid residueduringthe fire-extinguishing process. The facilityhousingthe GDIT Cloud data center system is staffed on a24 hourbasis by GDIT Cloud data center personnel. GDIT Cloud East: Fire suppression systems are in place. The system is a dry pipe, pre-action dual interlock system. Fully redundant environmental infrastructure includes UPS and generator protected power, redundant cooling and humidification, and state-of-the-art fire detection and protection systems. |

### PE-14 Temperature and Humidity Controls (L) (M) (H)

The organization:

1. Maintains temperature and humidity levels within the facility where the information system resides at [FedRAMP Assignment: consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments]; and

PE-14 (a) Additional FedRAMP Requirements and Guidance:   
Requirement: The service provider measures temperature at server inlets and humidity levels by dew point.

1. Monitors temperature and humidity levels [FedRAMP Assignment: continuously].

| PE-14 | Control Summary Information |
| --- | --- |
| Responsible Role: Facilities Manager | |
| Parameter PE-14(a): consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments | |
| Parameter PE-14(b): Continuously | |
| Parameter PE-14(b) Additional: The Facilities Manager maintains temperature and humidity levels within the facility where the information system resides at a level consistent with American Society of Heating, Refrigerating and Air-conditioning Engineers (ASHRAE) document entitled "Thermal Guidelines for Data Processing Environments measures temperature at server inlets and humidity levels by dew point. The GDIT Cloud West climate control system has been configured to maintainthe following climatethresholds: GDIT Cloud East The site has building management system that monitors and controls the temperature and humidity settings. Heating, Ventilation, and Air Conditioning (“HVAC”) system with high efficiency chilled water plant and on-site make-up water supply wells maintainthe following climatethresholds: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-14 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Facility Manager monitors temperature and humidity levels continuously as follows: GDIT Cloud West and East The monitoring system is built on APC’s StruxureWare Data Center Expert software. This software is not installed on an APC appliance device but is installed on a VM (out of band) located at the Westminster data center. The system is currently designed for a VLAN with 3 subnets at the following data centers: Westminster, CO; Manassas, VA, and Lawrence, KS. It sends an email to GDIT Cloud’s Cherwell ticketing system when conditions fall outside the required ranges specified in part a of this control. The NOC monitors the ticketing system 24x7 to respond to the alarms. Environmental monitoring equipment consists of the following: GDIT Cloud East Only COPT monitors environmental systems 24x7 from within the onsite Network Operations Center.. |
| Part b | Click or tap here to enter text. |

### PE-15 Water Damage Protection (L) (M) (H)

The organization protects the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

| PE-15 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-15 What is the solution and how is it implemented? |
| --- |
| There are two liquid leak sensors connected to each CRAC unit under the raised floor of the data center that will alarm at the CRAC unit within the data center and at the remote panel in the pump room. The facility housing the WOC has a secure water shutoff valve that will stop all water flow into the building in the event a situation warrants the water to be turned off to prevent damage. This area is locked and can only be accessed through the Westmoor Security (303-466-5588 during work hours or 720-334-0036 after hours). There is no automatic mechanism for implementing master water shutoff and valve activation. The 24/7 NOC Watch Desk has access to the dry pipe pre-action fire sprinkler riser that serves the fire sprinkler system in the data center and can shut off water flow to the data center in the event of inadvertent actuation that results in water flow. The GDIT building is geographically located in an area that is not subject to flooding. GDIT Cloud East: Water shut-off valve(s) are located in secure rooms that are one level below. |

### PE-16 Delivery and Removal (L) (M) (H)

The organization authorizes, monitors, and controls [FedRAMP Assignment: all information system components] entering and exiting the facility and maintains records of those items.

| PE-16 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-16: All information system components | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PE-16 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud is required to control information system-related items and maintain proper custodyofsuch items. All GDIT Cloud data center information system-related hardware, software,and firmwareenteringand exitingthe GDIT Cloud datacenter is authorized, monitored, and controlled. TheGDIT Cloud data center also maintains records of those items. The GDIT Cloud data center complies with this requirementas follows: Theintroduction or removal of cloud-related hardware, software, and firmwareis authorized bythe GDIT Cloud ChangeAdvisory Board (CAB) and is tracked through theuseofthe Cherwell configuration management system. Software, hardware, andfirmware physicallyintroduced to or removed from the data center are also recorded via the Cherwell Configuration Management Data Base (CMDB) located inside the GDIT Cloud data center. (See controls are MA-2and MA-3.) All changes to the GDIT Cloud data center software, hardware, or firmware are recorded by authorized personnel in the Cherwell Hardware/Software Inventory Database. (See control: CM-8.) All incoming and outgoing GDIT Cloud data center deliveries ormail that arrives at the facility are controlled bythe GDIT FacilitySecurity Officers. Information system-related items includinghardware, software, and firmware enteringthe facilityviathesemeans aretracked bythe systemused bythesecuritypersonnel in the facility. The GDIT Cloud data center information system-related items arepicked up and/ordelivered to authorized personnel only. Items delivered to and exiting from thedata center will beproperlyhandled through approved document management such aspropershippingdocuments obtained, item release/receipt forms, and propertysign-in log. GDIT Cloud East: All incoming and outgoing packages are tracked and require signatures for delivery. GDIT receives a monthly “GDIT - Delivery Log - October2014”. Perimeter gate Security Guards validate the delivery from a list of authorized deliveries. The Loading dock security guard monitors the delivery from the truck to the inside load dock area. Equipment is unwrapped before it is moved to the Cage. |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and
2. Reviews and updates the current:
   1. Security planning policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Security planning procedures [FedRAMP Assignment: at least annually].

| PL-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PL-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter PL-1(b)(1): at least every 3 years | |
| Parameter PL-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PL-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.14. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal Risk Assessment controls in the Cloud’s GDIT-OC-PRO-PL Planning Procedures. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### PL-2 System Security Plan (L) (M) (H)

The organization:

1. Develops a security plan for the information system that:
   1. Is consistent with the organization’s enterprise architecture;
   2. Explicitly defines the authorization boundary for the system;
   3. Describes the operational context of the information system in terms of missions and business processes;
   4. Provides the security categorization of the information system including supporting rationale;
   5. Describes the operational environment for the information system and relationships with or connections to other information;
   6. Provides an overview of the security requirements for the system;
   7. Identifies any relevant overlays, if applicable;
   8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and
   9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;
2. Distributes copies of the security plan and communicates subsequent changes to the plan to [Assignment: organization-defined personnel or roles];
3. Reviews the security plan for the information system [FedRAMP Assignment: at least annually];
4. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and
5. Protects the security plan from unauthorized disclosure and modification.

| PL-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PL-2(b): Management roles (System Owner; Director, Data Center; Technical Manager, Operations; Technical Manager, Engineering; Configuration-Change Manager; Security Operations Manager | |
| Parameter PL-2(c): at least annually]; | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | This ISSO has developed a security plan for the information system that: Is consistent with the organization’s enterprise architecture; Section 8.4 provides details on the system’s architecture. Explicitly defines the authorization boundary for the system; Section 8.2 describes and provides a diagram depicting the system’s authorization boundary. Describes the operational context of the information system in terms of missions and business processes; Section 8.1 describes the system’s function and purpose. Provides the security categorization of the information system including supporting rationale; Section 2 provides the information system categorization along with the rationale. Describes the operational environment for the information system and relationships with or connections to other information systems; Section 8.2 describes system components (operational environment) and section 10 describes system interconnections. Provides an overview of the security requirements for the system; Section 11 provides the minimum security requirements. Identifies any relevant overlays, if applicable; Not applicable. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and Sections 11.1 through 11.17 provide detailed information about all security controls in place and how they are implemented along with tailoring information. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation This SSP is reviewed at least annually and approved by the JAB. |
| Part b | The ISSO distributes copies of the security plan and communicates subsequent changes to the plan to Management roles (System Owner; Director, Data Center; Technical Manager, Operations; Technical Manager, Engineering; Configuration-Change Manager; Security Operations Manager) through email announcement that a new version of the SSP is available. The SSP is maintained on the access controlled internal SharePoint site and is posted to Cherwell as the official change to the document. This is captured in KA 11106 GDIT Cloud System Security Plan (11/28/2016) Note: The KA date is updated with the submission of this version of the document. |
| Part c | The Cloud ISSO reviews the security plan for the information system at least annually as part of continuous monitoring. The ISSO intiates the annual SSP reviewthrough the GDIT Cloud Security Calendar that is maintained on the GDIT Cloud SharePoint site. Changes to documentation are governed by the change management process and are approved by the CAB, and by ISSO and System Owner on the signature page of this document.. The results of the review are recorded both in the change/version section of the SSP and in the Cherwell ticket. |
| Part d | The Cloud ISSO updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. Any change in security controls must be approved by PMO prior to implementation and then documented in the GDIT Cloud SSP. Significant changes to the system may require the completion of a new GDIT Cloud A&A. The ISSO notifies the FedRAMP ISSO when any PMO-approved updates or changes to the SSP have been completed. All identified changes are submitted as change requests that are managed by the change management process. If approved, the changes to the document are managed by the configuration management process, which governs document version control. |
| Part e | To protect the GDIT Cloud System Security Plan from unauthorized disclosure and modification, the ISSO maintains the authorized version in the access controlled GDIT Cloud internal SharePoint site. Additionally, as updated versions of the SSP are released, the ISSO uploads them to the access controlled MAX.gov site for FedRAMP authorized systems. |

### PL-4 Rules of Behavior (L) (M)

The organization:

1. Establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
2. Receives a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system;
3. Reviews and updates the rules of behavior [FedRAMP Assignment: at least every three (3) years]; and
4. Requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated.

| PL-4 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PL-4(c): at least every three years | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PL-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO establishes and makes readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior with regard to information and information system usage through the GDIT Cloud Rules of Behavior (ROB). The current version of the GDIT ROB is maintained by the ISSO as an appendix to the GDIT Cloud SSP. |
| Part b | The ISSO maintains records of the Rules of Behavior on the secure GDIT Cloud SharePoint Site. A system access account cannot be created without a signed Rules of Behavior form, according to the GDIT Cloud Employee On-Boarding and Off-Boarding. Once signed by individuals, the signature page is scanned and sent to ISSO, who attaches the signed RoB to the on-boarding ticket. |
| Part c | The ISSO reviews and updates the Rules of Behavior (ROB) at least every three years according to the Continuous Monitoring program and Security Calendar or when there is a significant change. |
| Part d | The GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.14 requires individuals who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised/updated. |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and
2. Reviews and updates the current:
   1. Personnel security policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Personnel security procedures [FedRAMP Assignment: at least annually].

| PS-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PS-1(a): at least every three years | |
| Parameter PS-1(b)(1): at least annually | |
| Parameter PS-1(b)(2): The ISSO has documented the GDIT Cloud’s personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.14. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal Risk Assessment controls in the Cloud’s GDIT-OC-PRO-PS, Personnel Security Procedures. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| PS-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |
| Part b | Click or tap here to enter text. |

### PS-2 Position Categorization (L) (M)

The organization:

1. Assigns a risk designation to all positions;
2. Establishes screening criteria for individuals filling those positions; and
3. Reviews and revises position risk designations [FedRAMP Assignment: at least every three (3) years].

| PS-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PS-2(c): Annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud System Owner identifies categories for all positions and indicates a minimum need for personnel to have background checks. GDIT Cloud System Owner determines an employee’s risk designation based on job role and system access requirements. GDIT Cloud System Owner designates position at a high, moderate, or low risk level, as determined by the position's potential for adverse impact to the efficiency and integrity of the service. Typical Personnel Risk Classification Criteria is listed in the table below. |
| Part b | Assigning a risk designation to all positions and establishing screening criteria is required by GSA policy GSA IT Security Policy, GSA Order CIO P 2100.1G and procedures. Position Categorization and associated criteria for screening GDIT employees is consistent with 5 CFR 731.106(a) / OPM policy and guidance. The GDIT ISSO has decided to take a high water mark approach and screen all employees and contractors as though their job role carried a “high risk” and requires all our employees to be subject to a Background Investigation before hire date. The Screening Criteria are outlined below: Identification verification SSN verification Education verification National criminal file search Past employment verification Anything beyond these is driven by our additional customer requirements. |
| Part c | The ISSO and System Owner review and update position risk designations on an annual basis as part of the Continuous Monitoring program as dictated by the Security Calendar. The ISSO initiates the review in conjunction with the annual SSP review and update. The ISSO updates the roles and risk designations then sends the updated version to the System Owner for review and approval. |

### PS-3 Personnel Screening (L) (M) (H)

The organization:

1. Screens individuals prior to authorizing access to the information system; and
2. Rescreens individuals according to [FedRAMP Assignment: For national security clearances; a reinvestigation is required during the fifth (5th) year for top secret security clearance, the tenth (10th) year for secret security clearance, and fifteenth (15th) year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the fifth (5th) year. There is no reinvestigation for other moderate risk positions or any low risk positions].

| PS-3 | Control Summary Information |
| --- | --- |
| Responsible Role: HR | |
| Parameter PS-3(b): for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low risk positions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | HR screens all GDIT Cloud personnel before employment and access to Cloud resources. GDIT Cloud personnel screening involves a position description statement that is used in a requisition for services. The requisition determines the level of screening based on requirements that are mandatory. Each applicant goes through a process based on GDIT policy, HR-POL-401 Recruiting, Staffing, and Hiring and HR-POL-301 Background Investigations) to administer background investigations in full compliance with all federal and state statutes, including the Fair Credit Reporting Act (FCRA), Americans with Disabilities Act (ADA) and Title VII of the Civil Rights Act of 1964, each as amended. Background information, as described below, is collected to validate the accuracy of an individual’s past employment, education, and other relevant data to aid in determining the applicant's overall employability and help ensure the protection of the people, assets, property, and information of the organization. GDIT background investigations will include: Social Security Number or Immigration Registration Number (to be verified directly through DHS and SSA records) Verification of Identity for the last seven years (Name and Address) Education (all post-secondary degrees listed [or high school diploma if there is no post-secondary degree] including certifications/professional licenses, etc.) Employment History (minimum of seven years) including dates of employment, job title, prior employer, and reason for termination (if disclosed) Salary Verification (prior employer, if disclosed) Criminal History Check (Federal, State and County criminal convictions, for seven years), Juvenile records excluded Citizenship Status (citizenship status is verified by Security or Human Resources for positions where U.S. citizenship is a requirement) All GDIT Cloud personnel are screened as follows: Resume review Interviews: phone & in-person No GDIT Cloud personnel will be granted access until the background investigations have been completed. |
| Part b | GDIT HR conducts rescreening activities as required. GDIT Cloud management adheres to the following reinvestigation criteria: For national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for low risk positions. At a minimum, all staff go through a five-year public trust reinvestigation. |

### PS-4 Personnel Termination (L) (M)

The organization, upon termination of individual employment:

1. Disables information system access within [FedRAMP Assignment: same day];
2. Terminates/revokes any authenticators/credentials associated with the individual;
3. Conducts exit interviews that include a discussion of [Assignment: organization-defined information security topics];
4. Retrieves all security-related organizational information system-related property;
5. Retains access to organizational information and information systems formerly controlled by terminated individual; and
6. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].

| PS-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter PS-4(a): same day | |
| Parameter PS-4(c): security topics in accordance with the GDIT HR-POL-410, Separation from Employment and applies or defers to Corporate HR the appropriate steps in HR-FORM-410B, Out-Processing Checklist. | |
| Parameter PS-4(f)-1: System manager and ISSO within same day of termination | |
| Parameter PS-4(f)-2: A service request ticket is created by the System Manager in the GDIT Cloud Ticketing system to initiate the disabling of information system access for the individual being terminated. A System Administrator accesses the GDIT Cloud AD and disables the individual’s account(s) in accordance with the AC policies and procedures. The GDIT Cloud service request ticket is updated with the time of disablement and a list of all the accounts. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | A System Administrator accesses the GDIT Cloud MMS A&A systems and disables the individual’s account(s) in accordance with the AC policies and procedures. As stated in AC-2(h), all accounts for terminated or transferred personnel are deactivated within 24 hours and removed after review for removal by the GDIT Cloud ISSO. See KA 10588 Off Boarding form WCO Staff Member Checkout Checklist. This applies to both voluntary and involuntary termination. |
| Part b | The System Manager and/or HR conducts exit interviews in accordance with the GDIT HR-POL-410, Separation from Employment and applies or defers to Corporate HR the appropriate steps in HR-FORM-410B, Out-Processing Checklist . |
| Part c | GDIT recovers of organizational physical property (e.g., mobile devices) from the terminated individual. |
| Part d | GDIT retains access to organizational information and information systems formerly controlled by terminated individual through removal of the terminated individual's access credentials associated with all organizational facilities and information systems, change-of-ownership properties against information system objects to the terminated individual's immediate supervisor (or next level superior). |
| Part e | GDIT notifies System manager and ISSO within same day of termination. |
| Part f | Click or tap here to enter text. |

### PS-5 Personnel Transfer (L) (M)

The organization:

1. Reviews and confirms ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization;
2. Initiates [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
3. Modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
4. Notifies [Assignment: organization-defined personnel or roles] within [FedRAMP Assignment: within five days of the formal transfer action (DoD 24 hours)].

| PS-5 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PS-5(b)-1: transfer or reassignment actions | |
| Parameter PS-5(b)-2: immediately | |
| Parameter PS-5(d)-1: Sending Manager, Receiving Manager | |
| Parameter PS-5(d)-2: within five days of the formal transfer action | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | When personnel are reassigned or transferred to other positions, a request is sent to FedRAMP ISSO to obtain approval. The reassignment or transfer request form contains the following information: FedRAMP Control Condition: Reassignment or Transfer Person’s Name Reason Once approval is attained, we implement the reassignment or transfer through our ticketing process. |
| Part b | A service request ticket is created by the System Manager in the GDIT Cloud ticketing system to initiate the disabling of information system access for the individual being transferred. System Administrators access the GDIT Cloud AD systems and disables the individual’s account(s) in accordance with the AC policies and procedures. The GDIT Cloud service request ticket is updated with the time of disablement and a list of all the accounts. |
| Part c | GDIT transfers personnel to or from a project under the guidance of GDIT HR-POL-406 In-staff Transfers and Promotions: “The Sending and Receiving Manager re-assign responsibilities and ensure that job knowledge transfer takes place to ensure continuity of the function. The Sending and Receiving Manager ensure that access privileges are changed to reflect the new responsibilities.” Upon transfer, the System manager modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. A GDIT helpdesk ticket is opened upon completion of the administrative changes by HR so that the systems changes can then be enacted. These changes are implemented within five days. |
| Part d | The Service Desk notifies the sending manager and receiving manager within five days of the formal transfer action. |

### PS-6 Access Agreements (L) (M)

The organization:

1. Develops and documents access agreements for organizational information systems;
2. Reviews and updates the access agreements [FedRAMP Assignment: at least annually]; and
3. Ensures that individuals requiring access to organizational information and information systems:
   1. Sign appropriate access agreements prior to being granted access; and
   2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or [FedRAMP Assignment: at least annually].

| PS-6 | Control Summary Information |
| --- | --- |
| Responsible Role: HR | |
| Parameter PS-6(b): at least annually | |
| Parameter PS-6(c)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT HR develops and documents access agreements for GDIT Cloud organizational information systems that are signed as part of the on-boarding process. Each employee is required to read and sign a user agreement granting access to GDIT systems. |
| Part b | The ISSO reviews/updates the access agreements annually through the Continuous Monitoring program as dictated by the Security Calendar. The access agreements included in the annual review are as follows: Rules of Behavior (RoB) The review is conducted in conjunction with the annual review of the System Security Plan. If the RoB is updated as a result of the review, all GDIT personnel with access to the GDIT Cloud are required to read, understand, and sign the updated version of the document. Reviews and updates of the RoB are conducted in accordance with the requirements in PL-4. At this time, there are no other required access agreements for GDIT Cloud. |
| Part c | As part of the annual security training requirement, GDIT HR requires that employees sign an access agreement each year. Access agreements are maintained by GDIT HR. For employees that are assigned to the GDIT Cloud system, there is an additional annual requirement to read and sign the Rules of Behavior document. |

### PS-7 Third-Party Personnel Security (L) (M)

The organization:

1. Establishes personnel security requirements including security roles and responsibilities for third-party providers;
2. Requires third-party providers to comply with personnel security policies and procedures established by the organization;
3. Documents personnel security requirements;
4. Requires third-party providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within [FedRAMP Assignment: same day]; and
5. Monitors provider compliance.

| PS-7 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter PS-7(d)-1: The GDIT Cloud ISSO | |
| Parameter PS-7(d)-2: same day | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Through a work agreement signed by all 3rd parties, the System Manager provides the document and training to ensure all 3rd party personnel are assigned clear roles and responsibilities for the work period or performance. |
| Part b | Requires third-party providers to comply with personnel security policies and procedures established by the organization Through a signed work agreement, the System Manager provides the document and training to ensure all 3rd party personnel assigned an extended stay meet and conform to the FedRAMP security requirements. Those 3rd party personnel who visit for a single day or short period are assigned a GDIT Cloud staff person by the System Manager to escort and monitor the individual. |
| Part c | All third party personnel are subject to the same security requirements as GDIT Cloud personnel. GDIT HR maintains security compliance records of third party personnel. |
| Part d | The System Management requires that third-party providers notify the FSO of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within the same day. The FSO then notifies the ISSO. Contracted labor is treated as GDIT employees, otherwise they are considered as “visitors.” |
| Part e | – There are no additional compliance activities to monitor for this control. Third parties that count as visitors must be escorted and comply with requirements for visitors. Third parties which perform similar duties to regular employees count as employees for GDIT Cloud compliance.While GDIT Cloud can contractually request that contractor companies notify the FSO regarding Part d, we cannot review their records to identify if they failed to comply with that requirement. |

### PS-8 Personnel Sanctions (L) (M)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

| PS-8 | Control Summary Information |
| --- | --- |
| Responsible Role: HR | |
| Parameter PS-8(b)-1: roles defined in GDIT HR-POL-603 Performance Improvement and Corrective Actions | |
| Parameter PS-8(b)-2: time period defined in GDIT HR-POL-603 Performance Improvement and Corrective Actions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| PS-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | GDIT Cloud servers and supporting infrastructure are managed by GDIT personnel who are governed by GDIT’s technical security handbook which explicitly provides for sanctions (including termination) for failure to abide by security policies. Reference GDIT HR-POL-603 Performance Improvement and Corrective Actions. |
| Part b | The System Manager notifies the roles defined in GDIT HR-POL-603 Performance Improvement and Corrective Actions within time period defined when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. |

## Risk Assessment (RA)

### RA-1 Risk Assessment Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and
2. Reviews and updates the current:
   1. Risk assessment policy [FedRAMP Assignment: at least every three (3) years]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually].

| RA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter RA-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter RA-1(b)(1): at least every three years | |
| Parameter RA-1(b)(2): Assignment: at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| RA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s Risk Assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.14. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal Risk Assessment controls in the Cloud’s GDIT-OC-PRO-RA, Risk Assessment Procedures. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### RA-2 Security Categorization (L) (M) (H)

The organization:

1. Categorizes information and the information system in accordance with applicable Federal Laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and
3. Ensures the security categorization decision is reviewed and approved by the AO or authorizing official designated representative.

| RA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud ISSO completed a Security Authorization package to be authorized to operate at FIPS 199 Moderate impact level. Security categorization is a function of the data and not the system. Customer agencies/Departments must separately categorize their data in agreement with FIPS 199 and NIST 800-60, Rev. 1, Volumes 1& 2, Guide to Mapping Types of Information and Information Systems to Security Categories, to ensure that the security category of information types collected, processed, or supported by the GDIT’s Cloud offering do not exceed FIPS 199 Moderate impact for confidentiality, integrity, and/or availability. The GDIT Cloud FIPS 199 security categorization was conducted in accordance with FIPS 199 and NIST 800-60, Rev. 1, Volumes 1& 2, Guide to Mapping Types of Information and Information Systems to Security Categories. The categorization was review and approved by the System Owner and the GDIT Cloud Information System Security Officer. Customer Responsibility Customer agencies/Departments must separately categorize their data in agreement with FIPS 199 and NIST 800-60, Rev. 1, Volumes 1& 2, Guide to Mapping Types of Information and Information Systems to Security Categories to ensure that the security category of information types collected, processed, or supported by the GDIT Cloud offering do not exceed FIPS 199 Moderate impact for confidentiality, integrity, and/or availability. |
| Part b | Results are summarized in Section 2.1 of this plan. The overall security categorization has been assessed at the Moderate impact level for confidentiality, integrity, and availability respectively as determined in accordance with FIPS 199 guidelines. The security categorization process took into consideration supporting rationale for impact-level decisions and involved appropriate stakeholders and senior level organizational officials (program management, system owner) to review and approve (signature) the final security categorization activity. GDIT Cloud stakeholders have identified the following information types and rating for GDIT Cloud. Information Systems Information Type and Rating |
| Part c | The FIPS 199 Security categorization assessment was submitted for the review and approval of the FedRAMP ISSO and JAB. |

### RA-3 Risk Assessment (L) (M)

The organization:

1. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
2. Documents risk assessment results in [Selection: security plan; risk assessment report; [FedRAMP Assignment: security assessment report]];
3. Reviews risk assessment results [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs];
4. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and
5. Updates the risk assessment [FedRAMP Assignment: in accordance with OMB A-130 requirements or when a significant change occurs] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

RA-3 Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F

RA-3 (d) Requirement: Include all Authorizing Officials; for JAB authorizations to include FedRAMP.

| RA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter RA-3(b): Security Assessment Report | |
| Parameter RA-3(c): Every three years or when a significant change occurs | |
| Parameter RA-3(d): System owner, 3PAO | |
| Parameter RA-3(e): Every three years or when a significant change occurs | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager requires a FedRAMP PMO approved 3PAO conduct a security assessment to determine the security risk posture of the GDIT Cloud for a Provisional Authorization to Operate (P-ATO) that includes the assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. |
| Part b | The 3PAO documents the results of the security assessment in a Security Assessment Report (SAR). Upon completion of the assessment, the 3PAO provides the SAR to the FedRAMP PMO, GDIT Cloud System Owner, GDIT Cloud System Manager, and ISSO and uploads to the OMB MAX repository. |
| Part c | After an ATO is issued, the GDIT-OC-POL-1, GDIT Cloud Security Policy, requires that the ISSO reviews the risk assessment every three years or when a significant change occurs, as defined in NIST SP 800-37 rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems, Appendix F, Page F-7. |
| Part d | Upon completion of the assessment, the 3PAO provides the SAR to the FedRAMP PMO, GDIT Cloud System Owner, GDIT Cloud System Manager, and ISSO and uploads to the OMB MAX repository. |
| Part e | The ISSO updates the risk assessment at least every three years or when a significant change occurs or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system If any of the below listed events should occur, the ISSO updates the System Security Plan and other affected Security Authorization process documentation to reflect the new information system components, or new operating environment. The following changes to the information system or environment of the operations may also require a reauthorization of the information system: Addition or replacement of a major component or a significant part of a major system A change in security mode of operation A change in interfacing systems A significant change to the operating system or executive software, A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation A significant change to the physical structure housing the information system or environment of the information system that could affect the physical security described in the accreditation A significant change to the threat that could adversely affect the IaaS systems A significant change to the availability of safeguards, and/or A significant change to the user population. |

### RA-5 Vulnerability Scanning (L) (M) (H)

The organization:

1. Scans for vulnerabilities in the information system and hosted applications [FedRAMP Assignment: monthly operating system/infrastructure; monthly web applications and databases] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

RA-5 (a) Additional FedRAMP Requirements and Guidance:

Requirement: An accredited independent assessor scans operating systems/infrastructure, web applications, and databases once annually.

1. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
   1. Enumerating platforms, software flaws, and improper configurations;
   2. Formatting and making transparent, checklists and test procedures; and
   3. Measuring vulnerability impact;
2. Analyzes vulnerability scan reports and results from security control assessments
3. Remediates legitimate vulnerabilities; [FedRAMP Assignment: high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery], in accordance with an organizational assessment of risk; and
4. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

RA-5 (e) Additional FedRAMP Requirements and Guidance:

Requirement: To include all Authorizing Officials; for JAB authorizations to include FedRAMP.

RA-5 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Vulnerability Scanning Requirements

<https://www.FedRAMP.gov/documents/>

| RA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter RA-5(a): monthly operating system/infrastructure; web applications and databases | |
| Parameter RA-5(d): high-risk vulnerabilities mitigated within thirty days from date of discovery; moderate risk vulnerabilities mitigated within ninety days from date of discovery | |
| Parameter RA-5(e): Security Analysts, ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| RA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Security Engineers perform monthly scans on the GDIT Cloud operating system/infrastructure, web applications, and databases and when new vulnerabilities potentially affecting the system/applications are identified and reported. Additional details are included in Parts b through e. The monthly scan is initiated by the tools identified in part b to perform the activity automatically. The results of the scan are sent to a distribution list and stored in Cherwell In addition, an accredited independent assessor scans operating systems/infrastructure, web applications, and databases annually as part of the continuous monitoring program. The results of the independent assessor are recorded in the SAR and delivered to both GDIT Cloud management and the FedRAMP PMO. |
| Part b | Security Engineers employ tools that use standards for enumerating platforms, software flaws, improper configurations, formatting checklists and test procedures, and measuring vulnerability impact.. The tools are outlined in the table below. The tools combine the knowledge about many different operating systems and businesses to ensure up to data interoperability. The tools include functions to automate the scanning of the endpoints and delivery of the reports to a specified email distribution list. The tools are configured to download updates from the vendors to ensure the vulnerabilities that they scan include the latest discoveries. Security Engineers use these tools and the scan process to measure vulnerability impact by giving every flaw listed a CVSS score (1-10). The score is also translated in the POAM as low, moderate, or high. Reporting The scans produce a report that enumerates platforms, software flaws, and improper configurations that includes the flaw, the flaw source, and flaw description on every device. The GDIT Cloud ISSO uses the scan results to report the flaws to the FedRAMP PMO in an XML format upload a report to MAX every month. |
| Part c | Security Analysts analyze vulnerability scan reports and results from security control assessments to identify legitimate vulnerabilities. The results of the scans are retained and traceable by sending reports through the GDIT Cloud MMS Ticketing System to the appropriate owner of the technology. False positives are documented with a Deviation Request submitted to the FedRAMP JAB. Technology Engineers then determine the resolution and document the solution in the GDIT Cloud MMS Ticketing System ticket. The options for resolution are: Fix the vulnerabilities through the use of patches, new versions, and hot fixes. Mitigate the vulnerability in order to lessen the impact the vulnerability has on the system. Document the vulnerability in the POA&M ticket, Identify what action will be taken in the future to resolve the vulnerability or document the reason why the vulnerability might remain a residual risk. These resolutions are included in the POA&M list loaded in Max every month. When this process has been completed Security Analysts will compare the documented actions with the results of the next scheduled scan to validate what vulnerabilities have been mitigated and what vulnerabilities are still on the system. For more detail, see Part d. |
| Part d | GDIT Security Analysts review all vulnerabilities identified from automated scans and security assessments. Legitimate vulnerabilities are assigned a severity rating and response time. Vulnerabilities are added to the POA&M and are tracked along with a high level strategy and measurable milestones through resolution. High risk vulnerabilities are required to be remediated within 30 days of discovery, while all moderate risk vulnerabilities are required to be remediated within 90 days of discovery. The vulnerabilities and their remediation processes are tracked internally by System Administrators via Cherwell ticketing System while the GDIT Cloud ISSO tracks and reports all security assessment findings in the GDIT Cloud POA&M list. The primary means of detection are through internal program reviews, information security audits, security assessments, security impact analyses, and continuous monitoring activities. Documented weaknesses are used to determine the appropriate strategy for risk mitigation by defining clear, measurable milestones, the required resources, and target completion dates. The GDIT Cloud ISSO works with the respective Subject Matter Experts (SME) to correct the reported weakness and residual risks in a timely manner. The GDIT Cloud ISSO reviews the POA&M list to ensure that it is in compliance with the FedRAMP standards. |
| Part e | The ISSO shares information obtained from the vulnerability scanning process and security control assessments by distributing vulnerability information to all engineers throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). The distribution is accomplished by the following: GDIT Cloud MMS ticketing system; with searchable records Monthly meetings with the Principle Director, Cloud Operations; this role is the Risk Executive, see Tables 2-6 and 3-1. The FedRAMP PMO through the monthly POA&M list upload to MAX.gov. The internal distribution is as follows: SecurityCenter: Daniel Galecki, Peter Harroun, Scott Hinck, Brian Borland, Hunter McCallum, Aaron Hernandez, Matt Holcomb, Kyle Barton, Sara Goldberg, Kimberly Robinson, Ashley Current, Trevor Ouellette Acunetix, as documented in KA 11286, How To: FedRAMP - Web Application scanning : FedRAMP ISSO, OMNI Director of Engineering, ConMon Project Manager. |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls; and
2. Reviews and updates the current:
   1. System and services acquisition policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and services acquisition procedures [FedRAMP Assignment: at least annually].

| SA-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SA-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter SA-1(b)(1): at least every 3 years | |
| Parameter SA-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SA-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.7. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, system and services acquisition controls in the GDIT Cloud’s GDIT-OC-PRO-SA, System and Services Acquisition Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### SA-2 Allocation of Resources (L) (M) (H)

The organization:

1. Determines information security requirements for the information system or information system service in mission/business process planning;
2. Determines, documents, and allocates the resources required to protect the information system or information system service as part of its capital planning and investment control process; and
3. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

| SA-2 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud System Manager determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect GDIT Cloud through combined actions taken by the CIO, CISO and the Finance Department. Security requirements for the enterprise information systems in mission/business case planning are determined in the organization’s programming and budgeting documentation. Concurrently, program clients and GDIT Cloud Management allocate as part of the capital planning and investment control process, the resources required to adequately protect information systems. |
| Part b | The System Manager determines, documents, and allocates, as part of its capital planning and investment control process, all resources required to adequately maintain the confidentiality, integrity, and availability of GDIT Cloud. GDIT has assigned a dedicated Finance Manager to monitor and report all OPEX and CAPEX actual and forecasted expenses related to the GDIT Cloud to senior leadership. A multi-year forecast is reviewed monthly with the service delivery team; all elements of cost tied to the Cloud are reviewed in detail. The review includes delta reporting (Actuals vs forecast), as well as updates to our year recovery and cost projections.  The service delivery team communicates any and all future capital or investment needs to the Finance Manager during the monthly review; the Finance Manager documents those needs within a thorough P&L tracking tool. At least monthly, the Finance Manager and Service Delivery VP meet with the Sector GM, Divisional VP of Finance, and the Divisional Senior VP, to discuss any material changes to future OPEX/CAPEX projections.  Due to GDIT’s deep pool of available resources, both from a human capital and working capital perspective, senior leadership uses the monthly meeting to ensure the team has all needed resources to fully support GDIT Cloud build and O&M operations. |
| Part c | The System Manager creates an annual budget for each product line, of which the GDIT Cloud is one. These budgets are reviewed monthly at the executive level. The budgeting process includes developing and reviewing the budget at the individual line item level for third-party compliance and security audits. |

### SA-3 System Development Life Cycle (L) (M) (H)

The organization:

1. Manages the information system using [Assignment: organization-defined system development life cycle] that incorporates information security considerations;
2. Defines and documents information security roles and responsibilities throughout the system development life cycle;
3. Identifies individuals having information security roles and responsibilities; and
4. Integrates the organizational information security risk management process into system development life cycle activities.

| SA-3 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter SA-3(a): GDIT Cloud System Development Lifecycle (SDLC) Guide | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud Change Manager has developed the GDIT Cloud System Development Lifecycle (SDLC) Guide that includes as one of its objectives, “Ensure security requirements are incorporated during each phase of the life cycle” (section 1.4 Objectives). This SDLC framework enables oversight of the technology, security and quality aspects of projects and management of changes into the GDIT Cloud environment. The SDLC process is adaptive and provides for quick and efficient response to business needs as they arise, yet provides a consistent and stable framework for management of GDIT Cloud projects and tenants. |
| Part b | The System Manager defined the following GDIT Cloud system security roles and responsibilities: As listed in the GDIT Cloud System Development Lifecycle (SDLC) Guide, GDIT Cloud SDLC Board members comprise subject matter experts from GDIT Cloud with governance responsibility for the GDIT Cloud environment. These members are: GDIT Cloud Director (Board Leadership) GDIT Cloud NOC Manager GDIT Cloud SOC Manager GDIT Cloud Engineering Manager GDIT Cloud Change Manager Acceptance for a project to move forward through the SDLC is based on the majority vote by board members with Board Leadership having the authority to overrule the majority. Through each phase of the cycle, each of the board members has an information security responsibility. Thoughout the process, the GDIT Cloud ISSO is consulted to ensure security requirements are appropriately addressed. |
| Part c | The individual having security roles and responsibilities for GDIT Cloud is as follows: |
| Part d | GDIT Cloud System Development Lifecycle (SDLC) Guide, in section 1.4, includes the following security-related objectives: Improve the likelihood of successfully completing  GDIT Cloud projects based on scope, schedule, cost, and risks; Avoid/minimize risk to the production environment; Support the production and integration of quality technology products into the operational environment; Ensure security requirements are incorporated during each phase of the life cycle; |

### SA-4 Acquisitions Process (L) (M) (H)

The organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs:

1. Security functional requirements;
2. Security strength requirements;
3. Security assurance requirements;
4. Security-related documentation requirements;
5. Requirements for protecting security-related documentation;
6. Description of the information system development environment and environment in which the system is intended to operate; and
7. Acceptance criteria.

Additional FedRAMP Requirements and Guidance:

Guidance: The use of Common Criteria (ISO/IEC 15408) evaluated products is strongly preferred.   
See <http://www.niap-ccevs.org/vpl> or <http://www.commoncriteriaportal.org/products.html>.

| SA-4 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Once the Team identifies a requirement for an acquisition need, it employs a Common Criteria (ISO/IEC 15408) evaluation methodology that utilizes The National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme (NIAP/CCEVS) Website ( http://www.niap-ccevs.org/vpl ) to determine a product set that matches FedRAMP security requirements. In addition, the GDIT acquisition team uses the GDIT COTS Procurement Checklist to evaluate and determine the specific product to purchase. If a product is chosen for acquisition that is not listed as Common Criteria certified, then the security portion of the checklist is completed to determine if the product meets FedRAMP requirements. |
| Part b | GDIT Cloud achieves security strength requirements through the depth and detail of the access, auditing, hardening, and system integrity functional requirements in the checklist in Part a. |
| Part c | GDIT ensures that all components and sub-components within the authorization boundary of the systems are properly evaluated and meet GDIT Cloud functional security requirements and specifications prior to and/or during consideration for purchase. |
| Part d | GDIT has a documented procedure (GDIT – PUR-POL-1, Procurement ) to define the processes for acquiring technology infrastructure. The policy covers the acquisition of goods and services from the identification of a need to the resolution of any problems with the goods or services. It applies to all acquisitions for GDIT clients and customers, all employees who order goods and services, and all Purchasing personnel. The document will be provided (viewable) to the 3PAO auditor to validate its existence and to verify that it meets the security control. |
| Part e | All documentation is attached to the appropriate RFCs within its Cherwell ticket and listed in - the FedRAMP SharePoint folder under COTS Procurement Checklists. |
| Part f | GDIT ensures that all component’s and sub-components within the authorization boundary of the systems are properly evaluated. These components meet GDIT Cloud functional security requirements and specifications during development, test, and operations within the FedRAMP-authorized environments managed and maintained by GDIT Cloud. |
| Part g | GDIT ensures that all component’s and sub-components within the authorization boundary of the systems are properly evaluated and meet GDIT Cloud functional security requirements and specifications prior to and/or during consideration for deployment. This happens through the SDLC and/or the Change Management process. |

### SA-5 Information System Documentation (L) (M)

The organization:

1. Obtains administrator documentation for the information system, system component, or information system service that describes:
   1. Secure configuration, installation, and operation of the system, component, or service;
   2. Effective use and maintenance of security functions/mechanisms; and
   3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;
2. Obtains user documentation for the information system, system component, or information system service that describes:
   1. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms;
   2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
   3. User responsibilities in maintaining the security of the system, component, or service;
3. Documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and [Assignment: organization-defined actions] in response;
4. Protects documentation as required, in accordance with the risk management strategy; and
5. Distributes documentation to [Assignment: organization-defined personnel or roles)].

| SA-5 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter SA-5(c): creates documentation in-house | |
| Parameter SA-5(e): System Managers, developers, testers, administrators, users | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SA-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Manager maintains, protects (as required), and makes available (unless defined as not available) to authorized personnel (FedRAMP PMO) documentation as required by FedRAMP, that includes the following: Security Authorization Package Related Documentation Secure Configuration, Installation, and Operation (Configuration Management Plan) Security Roles and Responsibilities Security Plan Risk Assessment Report Component Inventory (Hardware/Software) Configuration Profiles (Baselines) Incident Response Plan Vendor Documentation of Hardware/Software Functional Requirements or Specifications Control Tailoring Workbook Template (CTWT) MOU/MOA/USA/SLAs Rules of Behavior FIPS 199 Categorization Control Implementation Summary (CIS) Contingency Plan (including Business Impact Analysis) Contingency Plan Test Results Security Assessment Report Vulnerability Scan Analysis Report Incorporated into Risk Assessment Report E-Authentication Threshold Analysis Privacy Impact Assessment and Questionnaire Plan of Action and Milestones Standard Operating Procedures Authorization to Operate Verification Reviews/Site Inspections Continuous Monitoring Plan Since GDIT Cloud system was designed using COTS products. Documentation that describes hardware and software functionality and security is readily available from the vendors from a technical perspective; therefore, GDIT Cloud has not experienced any instances where documentation has not been available or nonexistent.  These guides provide authorized personnel information about security configurations, acceptable system use policy (e.g. Rules of Behavior), and system functionality, which helps administrative users use the system more securely |
| Part b | COTS vendor documentation is obtained which describes secure use of system hardware and software, the use of security functions/features, and methods for interacting with system components. Vendor documentation is included in the Cloud Services SharePoint site. Users are also provided the GDIT Cloud Rules of Behavior by the ISSO.  The ROB describes acceptable system use policy and the security responsibilities for protecting system components and customer data. Documentation such as ROB, Incident Response Plan, and Contingency Plans were developed to identify each organization’s security role and the security roles of certain individuals.  In particular, that ROB was developed to describe security responsibilities of users with different roles. |
| Part c | Since both System Administration and user documentation are available and current at all times, there is no need to document failed attempts to acquire documentation. However, if a person were to have trouble locating documentation, a ticket could be created at the Service Desk and tracked to closure through SOP. One strategy would be to create the documentation in-house. |
| Part d | The Change Manager protects documentation as required, in accordance with the risk management strategy as a CI in the CM repository through the Change Management Policies and Procedures. |
| Part e | GDIT Cloud documentation is distributed to system managers, testers, administrators, and users through a common and accessible SharePoint site. |

### SA-9 External Information System Services (L) (M) (H)

The organization:

1. Requires that providers of external information system services comply with organizational information security requirements and employ [FedRAMP Assignment: FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
2. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
3. Employs [FedRAMP Assignment: Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored] to monitor security control compliance by external service providers on an ongoing basis.

Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> Continuous Monitoring Strategy Guide  
<https://www.FedRAMP.gov/documents>

Guidance: Independent Assessors should assess the risk associated with the use of external services. See the FedRAMP page under Key Cloud Service Provider (CSP) Documents>FedRAMP Authorization Boundary Guidance

| SA-9 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SA-9(a): FedRAMP Security Controls Baseline(s) if Federal information is processed or stored within the external system | |
| Parameter SA-9(c): Federal/FedRAMP Continuous Monitoring requirements must be met for external systems where Federal information is processed or stored. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. Date of Authorization | |

| SA-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | At this time there are no external service connections with any third-party vendors. Should the need arise, the change will be coordinated with the FedRAMP to determine the impact to the security authorization package and ensure appropriate flow down of all the GDIT Cloud security requirements to the third-party vendor. |
| Part b | At this time there are no external service connections with any third-party vendors. Should the need arise, the change will be coordinated with the FedRAMP to determine the impact to the security authorization package and ensure appropriate flow down of all the GDIT Cloud security requirements to the third-party vendor. |
| Part c | At this time there are no external service connections with any third-party vendors. Should the need arise, the change will be coordinated with the FedRAMP to determine the impact to the security authorization package and ensure appropriate flow down of all the GDIT Cloud security requirements to the third-party vendor. |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
2. Reviews and updates the current:
   1. System and communications protection policy [FedRAMP Assignment: at least every three (3) years]; and
   2. System and communications protection procedures [FedRAMP Assignment: at least annually].

| SC-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SC-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter SC-1(b)(1): at least every 3 years | |
| Parameter SC-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SC-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.7. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, system and services acquisition controls in the GDIT Cloud’s GDIT-OC-PRO-SC, System and Communications Protection Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### SC-5 Denial of Service Protection (L) (M) (H)

The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards].

| SC-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter SC-5-1: ; Cisco Defined FirePower Intrusion policy of “Balanced Security and Connectivity” | |
| Parameter SC-5-2: organization-defined security safeguards | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-5 What is the solution and how is it implemented? |
| --- |
| The CISCO ASA Firewall/IDP functionality helps identify DDOS attacks and also prevents any high volume attacks on blocked ports. We also coordinate very closely with our upstream service providers for DDOS attack detection, coordinated response, and mitigation. The DDOS threats that are managed by the ASA firewalls are documented by Cisco at this link: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html#anc1 GDIT Cloud sets the ASA firewalls to Basic Threat Detection and Advanced for ACLs, as referenced in the link. This is the default. GDIT Cloud may modify the thresholds afterwards as needed. GDIT Cloud also uses the Firepower IPS to identify additional DDOS threats via the cisco policy of “Balanced Security and Connectivity”. DDOS signatures that are triggered are fed into the GDIT Cloud MMS SIEM for processing and storage. Where appropriate those signatures generate alerts that are processed by the GDIT Cloud Operations team. |

### SC-7 Boundary Protection (L) (M) (H)

The information system:

1. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and
2. Implements subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
3. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture.

| SC-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-7(b): physically and logically | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-7 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Network Engineers monitor and control communications at the external boundary of the GDIT Cloud and at key internal boundaries within the system. External Boundary: The CISCO ASA Border firewalls represent the managed interface to external networks. Network Engineers apply the appropriate Access Control Lists (ACLs) to ensure that traffic flow communications are directed to the approved Ports, Protocols, and services. Key Internal Boundaries: The Traffic Controller Firewall is the inside boundary protection and has three contexts (Virtual Firewalls): Tech Services, Customers 1, and Customers 2. The Traffic Controller Firewall directs traffic into the appropriate VLAN. Network Engineers configure each customer to have its own set of VLANs on the firewall. At the VM level, the GDIT Cloud enforces a policy of no direct VM-to-VM communication on the public interfaces unless mediated by the CISCO ASA internal firewalls. This communication is prohibited through the imposition of ACL restrictions. The firewall is configured to Deny IP any any log and no VLAN-to-VLAN communication is permitted. To monitor the communications, Network Engineers installed IDS modules on the CISCO ASA Firewalls, which inspect the content permitted by Access Control Lists against a list of known signatures. The signatures are updated on a weekly basis. The alerts from the IDS are fed into the GDIT Cloud MMS for review. |
| Part b | Network Engineers implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks through the Traffic Controller Firewall that is the inside boundary protection and which has three contexts (Virtual Firewalls): Tech Services, Customers 1, and Customers 2. The Traffic Controller Firewall directs traffic into the appropriate VLAN. Network Engineers configures each Customer with its own set of VLANs on the firewall. This includes a the GDIT Cloud policy enforcement of no direct VM-to-VM communication on the public interfaces unless mediated by the CISCO ASA internal firewalls, which is prohibited through the imposition of ACL restrictions, Deny IP any any log, and no VLAN-to-VLAN communication. |
| Part c | The GDIT Cloud network team manages the Border Guard firewall by the GDIT Cloud through a set of commands to implement IPsec tunnels, VPNs, and rules that define ports and protocols to external networks. The GDIT Cloud security architecture requires that all external connecting communications have a Border Guard firewall as its boundary protection. The GDIT Cloud connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with organizational security architecture that includes t wo distinct networks: Internal: Connects the data centers to form the Cloud External: Connects the Cloud to the Internet All external access passes through the GDIT Cloud Border Guard. The GDIT Cloud leverages the RSA SecureID infrastructure to provide Authentication and Authorization services as identified in the AC controls. |

### SC-12 Cryptographic Key Establishment & Management (L) (M) (H)

The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].

SC-12 Additional FedRAMP Requirements and Guidance:

Guidance: Federally approved and validated cryptography.

| SC-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter SC-12: organization-defined requirements for key generation, distribution, storage, access, and destruction]. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-12 What is the solution and how is it implemented? |
| --- |
| Network Engineers establish and manage cryptographic keys for required cryptography employed within the GDIT Cloud, as follows: Key generation, distribution, storage, use, destruction and archiving are automatically implemented in the FIPS-140-2 compliant firewalls and IPSEC VPN Border Guard system. GDIT Cloud Staff access the GDIT Cloud ticketing system’s webserver through industry standard browsers and HTTPS using TLS 1.0 or higher. The GDIT Cloud employs FIPS 140-2 validated encryption modules and supports FIPS-approved ciphers. No users are authenticated using personal certificates. Customer Responsibility Customers are responsible for securing their own cryptography keys. The Cloud provides FIPS 140-2 validated crypto modules to secure transmission and provides confidentiality and integrity. |

### SC-13 Use of Cryptography (L) (M) (H)

The information system implements [FedRAMP Assignment: FIPS-validated or NSA-approved cryptography] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

| SC-13 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-13: FIPS-validated | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-13 What is the solution and how is it implemented? |
| --- |
| The respective technology engineers implement required cryptographic protections using cryptographic modules within the technology components that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The GDIT Cloud uses encryption to protect the integrity and confidentiality of information in transmission using TLS, SSL, SSH, SFTP, and VPN protocols and technologies. The respective technology engineers employ FIPS 140-2 validated encryption modules and supports FIPS-approved ciphers. The respective technology engineers disable ciphers and protocols that do not meet FIPS 140-2 requirements where allowed by the vendor. These technologies are made available to all customers for any application requirements. Customer Responsibility SC-13, SC-13(1) Customers are responsible for configuring their web browsers, mobile devices, etc., to enable communications through encryption. Customers must implement the required FIPS 140-2 encryption for data transmitted. In addition, Customers are responsible for implementing the Transmission Integrity, Transmission Confidentiality, Use of Cryptography, and Session Authenticity controls for the applications that Customers establish within their Virtual Machine environments. |

### SC-15 Collaborative Computing Devices (L) (M) (H)

The information system:

1. Prohibits remote activation of collaborative computing devices with the following exceptions:[FedRAMP Assignment: no exceptions] and
2. Provides an explicit indication of use to users physically present at the devices.

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter SC-15(a): No exceptions | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | There are no Collaborative Computing Devices attached to the GDIT Cloud IaaS. Within each facility there are IP cameras to monitor access to data center equipment. Images from these are transmitted out-of-band to displays in the west NOC/SOC. |
| Part b | The security cameras are not connected to the IaaS network, but are part of our security program to identify intruders. Signs are posted in all areas where IP cameras are in use, and the cameras present a physical indicator when they are active. |

SC-15 Additional FedRAMP Requirements and Guidance:

Requirement: The information system provides disablement (instead of physical disconnect) of collaborative computing devices in a manner that supports ease of use.

| SC-15 Req. | Control Summary Information |
| --- | --- |
| Responsible Role: Req. 1 There are no Collaborative Computing Devices attached to the GDIT Cloud IaaS. The security cameras are not connected to the IaaS network, but are part of our security program to identify intruders. Signs are posted in all areas where IP cameras are in use, and the cameras present a physical indicator when they are active. | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-15 What is the solution and how is it implemented? | |
| --- | --- |
| Req. 1 | Click or tap here to enter text. |

### SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H)

The information system:

1. Provides additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and
2. Provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

| SC-20 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-20 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud provides Secure Name-Address Resolution by utilizing DNSSEC for its domains both internally and externally. External DNSSEC is enabled through our external provider GoDaddy, which enables DNSSEC for our public DNS resolution. Internal Internally GDIT Cloud DNS services are built upon Windows 2012 DNS services, which support Secure Name-Address Resolution through domain signing. Remote Internet clients cannot access the GDIT Cloud DNS servers, which are only used by internal Cloud systems (IaaS and Customers). Windows 2012 DNS provides extensive support for DNSSEC and all GDIT Cloud domains are signed using RSA/SHA-256 with 2048 bit key size. Any requests that can’t be resolved internally are sent to Google’s Public DNS server for resolution. Google public DNS is a validating, security-aware resolver and all responses from DNSSEC signed zones are validated unless clients explicitly flag requests to disable validation. The use of DNSSEC internally enables local Cloud systems to obtain origin authentication from the service and a level of integrity verification assurances for the host/service name to network address resolution information obtained through the service. The GDIT Cloud will utilize DNS services inside the FedRAMP boundary for resolution when required for the tasks associated with the actions of the Business Portal (i.e. provisioning, reporting, etc.).  The virtual machines that are provisioned from the portal will utilize DNS services outside the FedRAMP boundary.  Neither the GDIT Cloud DNS services inside the FedRAMP boundary nor the GDIT Cloud DNS services outside the boundary are accessible outside the GDIT Cloud itself. Customer Responsibility Since GDIT Cloud DNS is used only for namespaces internally within the Cloud, providing external facing Secure Name-Address Resolution for customer domains is a customer responsibility. GDIT Cloud can support for providing DNSSEC signed domains for internal use if requested. |
| Part b | GDIT Cloud DNS services are built upon Windows 2012 DNS. All current internal DNS zones are Active-Directory integrated and signed through DNSSEC. Windows 2012 DNS supports the verification of child zones and verifying the chain of trust among parent and child domains. If new child zones are required, GDIT Cloud Administrators initiate a change process to re-sign the parent zone. Customer Responsibility Since GDIT Cloud DNS is used only for namespaces internally within the Cloud, providing external facing Secure Name-Address Resolution for customer domains is a customer responsibility. This includes when operating as part of a distributed hierarchical namespace.  Customer Agencies are responsible for providing the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. |

### SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H)

The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

| SC-21 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-21 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud DNS client uses authenticated channels to recursive resolvers (provided by Google) who perform such validations. The DNS forwarding supports DNSSEC. Google is a trusted validation provider to GDIT Cloud IaaS. Google performs verification on the name/address resolution responses as the authoritative source. |

### SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H)

The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

| SC-22 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-22 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud provides name/address resolution services that are fault-tolerant. Each Data Center has two DNS resolution services. The GDIT Cloud has implemented only internal DNS resolution services. Customer Responsibility DNS and DNSSEC are the responsibility of the client. It is the client’s reasonability to ensure their virtual name/address resolution systems: Provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. When operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. Performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems. Provide name/address resolution service for an organization and are fault-tolerant and implement internal/external role separation. |

### SC-39 Process Isolation (L) (M) (H)

The information system maintains a separate execution domain for each executing process.

| SC-39 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SC-39 What is the solution and how is it implemented? |
| --- |
| Network Engineers maintain a separate execution domain for each executing process through the VMware hypervisor , as follows: Secure isolation of virtual machines at the virtualization layer. This includes secure instruction isolation. The hypervisor primarily is the management interface to the hardware primitives. Isolation of CPU, memory, and I/O is done at a hardware level, with the hypervisor managing how much of the hardware resources a virtual machine can use, similar to a choreographer or traffic officer. This part of the hypervisor is called the virtual machine monitor (VMM). With the ability to leverage these CPU extensions, the attack surface of the hypervisor shrinks considerably. Intel VT-x and AMD-V both enable a VMM to give the CPU to a virtual machine for direct execution—an action called a virtual machine entry—until the time the virtual machine attempts to execute a privileged instruction. At that point, the virtual machine execution is suspended and the CPU is given back to the VMM—an action called a virtual machine exit. The VMM then follows the classic mainframe-era approach, inspecting the virtual machine instruction that caused the exit as well as other information provided by the hardware in response to the exit. With the relevant information collected, the VMM emulates the virtual machine privileged instruction against the virtual machine state and then resumes execution of the virtual machine with another virtual machine entry. Memory pages that are identical in two or more virtual machines are stored once in the host system’s RAM, and each of the virtual machines has read-only access. Such shared pages are common, for example, if many virtual machines on the same host run the same OS. As soon as any one virtual machine attempts to modify a shared page, it gets its own private copy. Because shared memory pages are marked copy-on-write, it is impossible for one virtual machine to leak private information to another through this mechanism. Transparent page sharing is controlled by the VMkernel and VMM and cannot be compromised by virtual machines. It can also be disabled on a per-host or per–virtual machine basis. Each virtual machine is isolated from other virtual machines running on the same hardware. Virtual machines share physical resources such as CPU, memory, and I/O devices; a guest OS in an individual virtual machine cannot detect any device other than the virtual devices made available to it. A virtual machine cannot map to a device that has not been preassigned. A virtual machine is incapable of mounting another virtual machine’s disk unless the disk has been explicitly assigned to both virtual machines in the management console; for example, VMware vCenter™ or ESXi. |

## System and Information Integrity (SI)

### SI-1 System and Information Integrity Policy and Procedures (L) (M)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
   1. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
2. Reviews and updates the current:
3. System and information integrity policy [FedRAMP Assignment: at least every three (3) years]; and
4. System and information integrity procedures [FedRAMP Assignment: at least at least annually].

| SI-1 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SI-1(a): System Manager, Project Manager, System Architect, Configuration-Change Manager, ISSO | |
| Parameter SI-1(b)(1): at least every 3 years | |
| Parameter SI-1(b)(2): at least annually | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific) | |

| SI-1 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The ISSO has documented the GDIT Cloud’s system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance in the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.7. The ISSO will review and update this policy as required or at least annually. The ISSO has developed specific procedures for implementing GDIT Cloud’s formal, system and services acquisition controls in the GDIT Cloud’s GDIT-OC-PRO-SI, System and Information Integrity Procedures. This procedure is reviewed and updated as required or at least annually. All procedures are stored in a GDIT Cloud SharePoint site and version control is maintained. |
| Part b | The ISSO reviews and updates the policy and procedure as required or at least annually. Both the policy and procedures documents are managed by the change management process. Therefore, the review process is as follows: Knowledge Manager receives an automated notification when the Knowledge Article (KA), with associated policy is 30 days out from annual review. Knowledge Manager assigns the review to the ISSO and places the KA in the review queue in the tool. During the review, if the ISSO needs to make an update to the KA, the document change process is followed: The knowledge manager unlocks the baseline version of the document from the CMDB and sends to the ISSO The ISSO updates the document and submits a change request, which goes through CAB approval. After CAB approval the document is sent to the knowledge manager The Knowledge Manager locks the new baseline word document and attaches it to the CI record in the CMDB The Knowledge Manger creates a PDF from the word document and attaches it to the associate Knowledge Article. The Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### SI-2 Flaw Remediation (L) (M) (H)

The organization:

1. Identifies, reports, and corrects information system flaws;
2. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
3. Installs security-relevant software and firmware updates within [FedRAMP Assignment: thirty 30 days of release of updates] of the release of the updates; and
4. Incorporates flaw remediation into the organizational configuration management process.

| SI-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SI-2(c): Within 30 days of release of updates | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Security Engineers identifies, reports, and corrects information system flaws, as follows: GDIT Cloud Security analysts identify system flaws using the following means: Detection of vulnerabilities or other problems following a vulnerability scanner definition update Scans are run using the new plugin updates. Flaws are identified if a component tests positive with the new plugins. Indications and warning alert messages from United States Computer Emergency Readiness Team (US-CERT) Security Engineers consult the US-CERT website and also receive email notifications from the site. Reports from Vendors Vendors periodically send emails on threats, vulnerabilities, and flaws that have been discovered on their products. Proactive scans based on news of current threats and system issues. Ad-hoc scans can be run at any time as needed in addition to the scheduled scans. The tool used to perform the scan is Security Center. Security Analysts report the flaws by entering a ticket into the GDIT Cloud ticketing system for submission and tracking of incidents, requests, problems, and changes during the systems lifecycle, including flaws uncovered in scanning. The ticket is assigned to the appropriate Engineer, depending on the component affected. The Engineer corrects the flaw and sends the ticket back to the CAB for closure. In addition, GDIT Cloud subscribes to vendor security notices of vendors that supplied the various system components that are received by System Administrators. These notices detail vendor identified software defects that result in patches to operating systems, applications, and device firmware. The following are the vendors’ websites/advisories to whom the System Administrators subscribe: Cisco Security Advisories and Alerts (https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day\_sir#~Vulnerabilities ) Microsoft Technical Security Notifications ( https://technet.microsoft.com/en-us/security/dd252948 ) Tenable Product Security Advisories ( http://www.tenable.com/security ) SANS Internet Storm Center ( https://isc.sans.edu ) The Security Engineers make changes to the system to correct the flaws by following the change management process as governed by the GDIT Cloud Change Management Process and Procedures Guide, section 13. |
| Part b | The GDIT Cloud employs a process to test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation, as follows: System Administrators carefully evaluate patches, hot fixes and service packs released from vendors in relation to their impact on and relevance to the GDIT Cloud IaaS environment. Before patches are implemented in production, patches are tested in the test environment by first deploying the patches and verifying the system continues to function. Then a security scan is performed on the impacted system post deployment. Details in KA 10595, GDIT Cloud Patching. If a patch fails testing, the system is restored to its previous version. The System Administrators work to determine a root cause. If the root cause can be determined and remediated without system impact, the patches are presented to the CAB for approval. If the patch cannot be deployed without negative system impact, the ISSO is informed, who further investigates to determine if a deviation request is necessary. Patches are presented to the Change Advisory Board (CAB) for review at their normally scheduled meetings. Patch recommendations are then approved to the CAB via the GDIT Cloud ticketing system for approval to proceed with the implementation of the patches. In the event a set of patches is not CAB approved, the CAB informs the requester of the reason for rejection. If more information is required in the request, this can be stated in the reason for rejection; once the information is added to the request it can be accepted as normal. (GDIT Cloud Change Management Process and Procedures Guide). |
| Part c | The Security Engineers install security-relevant software and firmware updates within 30 days of release of updates of the release of the updates, as follows: System Administrators perform patch management for the GDIT Cloud in accordance with procedure and within 30 days of release of updates. Patches are routinely evaluated for applicability and relevant patch sets are tested and installed during routine system maintenance. In addition, patches are installed on an emergency basis to remediate critical risks. |
| Part d | The Configuration-Change Manager incorporates flaw remediation into the organizational configuration management process, as follows: System administrators use GDIT Cloud ticketing system for submission and tracking of incidents, requests, problems, and changes to the baseline as defined in the GDIT Cloud Service Asset and Configuration Management Process and Procedures Guide. All change to the system baseline is governed by the GDIT Cloud Change Management Process and Procedures Guide. If the flaw requires an immediate change to the system, the GDIT Cloud follows the ‘emergency change’ process described in the “[Emergency change is a] change that must be introduced as soon as possible, for example, to resolve or avoid a Major Incident that has high impact or severe degradation on the operation of the managed environment, or a priority security event such as implementing a security patch that is vital to business/mission effectiveness. An Emergency Change is implemented within a timeframe that does not allow normal change review (and therefore the Emergency Change may not be fully documented until after-the-fact). Emergency changes are submitted to the Emergency Change Advisory Board (ECAB) for approval. RFCs are declared emergencies at the recommendation of the Change Requester and upon concurrence with either the Change Manager or Deputy Change Manager (on behalf of the Change Manager), or the Engineering Manager, or the Westminster Data Center Manager.” Customer Responsibility The Customer agency is responsible for identifying, reporting, and correcting system flaws for operating systems and applications under their control. Customers are responsible to test software updates related to flaw remediation for effectiveness and potential side effects on customer information systems before installation; and incorporating flaw remediation into the organizational configuration management process. |

### SI-3 Malicious Code Protection (L) (M)

The organization:

1. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code;
2. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures;
3. Configures malicious code protection mechanisms to:
   1. Perform periodic scans of the information system [FedRAMP Assignment: at least weekly] and real-time scans of files from external sources at [FedRAMP Assignment: to include endpoints] as the files are downloaded, opened, or executed in accordance with organizational security policy; and
   2. [FedRAMP Assignment: to include alerting administrator or defined security personnel] in response to malicious code detection; and
4. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

| SI-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers. Security Engineers | |
| Parameter SI-3(c)(1)-1: at least weekly | |
| Parameter SI-3(c)(1)-2: Assignment to include endpoints | |
| Parameter SI-3(c)(2): to include alerting administrator or defined security personnel | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The Network Engineers employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code, as follows: The GDIT Cloud Border Guard employs Cisco Firepower to review incoming and outgoing traffic from the Internet. GDIT Cloud Border Guard Firepower sends the output of its real-time scans to the GDIT Cloud MMS SIEM where a Severity 1 alert is configured to alarm if the scan detects infected files. The alert generates a ticket in the ticketing system for Security Analysts investigation and if necessary IR action. All Microsoft and Red Hat servers include Symantec Endpoint Protection for host-based antivirus, browser protection, intruder prevention, download protection, and host based firewall countermeasures. Symantec endpoint protection conducts both real-time scanning of active files in use as well as a comprehensive system scan every 24 hours. The Symantec Endpoint Manager sends the alert of any identified malware in real-time or daily scans, to the GDIT Cloud MMS SEIM where a Severity 1 alert is configured to alert. The alert generates a ticket in the ticketing system for Security Analysts investigation and if necessary IR action. In addition to Symantec, Windows hosts include the Microsoft Enhanced Mitigation Experience Toolkit (EMET) suite of products. EMET includes the Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Structured Exception handler Overwrite Protection (SEHOP) modules employing Microsoft best practices for securing the operating system by how it interacts with applications. |
| Part b | The GDIT Cloud Border Guard IDS receives updates automatically to its signature library typically once per week, more frequently if CISCO release signatures more frequently for instances such as zero day attacks. GDIT Cloud MMS host-based protection AV is configured to automatically download and update its definitions from update servers that are within the GDIT Cloud IaaS. Those definitions are downloaded and installed weekly. Cisco Security Manager (CSM) downloads IDS signatures as they become available from the vendor. The Security Engineer manually tests these signatures for flaws, then manually uploads them to the Cloud Border Guard IDS. The ticket systems generates a periodic ticket initiate this weekly action. Updates can be applied more frequently if required by heightened threat levels. |
| Part c | Malicious code protection mechanisms come in two forms: 1) Network based, and 2) Host based. Network Based GDIT Cloud Border Guard has an Intrusion Detection System (IDS) set to alert on malicious traffic as it basses the boundary. The IPS operates scans in real time and sends alerts the SIEM. Host Based Symantec endpoint protection conducts both a comprehensive system scan every 24 hours as well as real-time scanning of active files in use during file download, file opening of file execution. What Happens if Malicious Code is Detected? The Symantec Endpoint Manager sends the alert of any identified malware in real-time or daily scans, to the GDIT Cloud MMS SEIM where a Severity 1 alert is configured to alert. The alert generates a ticket in the ticketing system for Security Analysts investigation and if necessary IR action. |
| Part d | Before taking any action from an alert, Security Analysts validate that the signature is not a false positive prior to any action that may impact the operational status of the system. The alert validation process is as follows: For GDIT Cloud Border Guard IDS alerts: Review the source and destination to identify the types of systems involved and review the alert details to see if they describe the systems involved. If not, the alert is flagged as false positive and documented in the ticket and elevated to Security Operations Manager for approval. If the systems involved match the alert type, the OS version / patch level / application are validated to determine if the system is vulnerable. If all these are a negative, then the alert is flagged as a false positive. For GDIT Cloud MMS host-based protection Anti-Virus: The files involved are cross-referenced with other maintenance activities on the system to identify if this is an expected alert. For GDIT Cloud MMS host-based protection: There are many directories known to have high rates of change for legitimate reasons, and those are ignored in the scans. If an alert is generated, the file type and directory structure are identified and researched to validate if the alert is against a file path / file that typically has a low or no rate of change (such as OS binaries). The alerts are cross-referenced with patching activities and other maintenance activities against that information system component. Handling False Positives As described above, each alert is reviewed to determine whether it is legitimate or a false positive. If it is determined that the alert is a false positive: The alert is documented in Cherwell as a False Positive The ticket is raised to management attention The following actions are performed: Stop the Incident Response process because it is generating a False Positive Identify the rule that generated the False Positive Contact the vendor to change technology signature or rules so that changes can be made to vendor updates. Make changes to in-house exceptions in accordance with Change management procedures and approvals. Potential Impact to Availability of the System Because the analysis of all alerts incorporates False Positive determination before responsive action is taken, there is no negative impact to system availability. |

### SI-4 Information System Monitoring (L) (M) (H)

The organization:

1. Monitors the information system to detect:
   1. Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and
   2. Unauthorized local, network, and remote connections;
2. Identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods];
3. Deploys monitoring devices (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;
4. Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;
5. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information;
6. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and
7. Provides [Assignment: organization-defined information system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].

SI-4 Additional FedRAMP Requirements and Guidance:

Guidance: See US-CERT Incident Response Reporting Guidelines.

| SI-4 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analysts | |
| Parameter SI-4(a)(1): ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; identify irregularities or anomalies that are indicators of a system malfunction or compromise | |
| Parameter SI-4(b): configure platforms to look at the incoming log and trap stream and perform correlation on words, phrases, event codes and raise notifications to the GDIT Cloud MMS Ticketing system where Security Analysts review | |
| Parameter SI-4(g)-1: monitoring information | |
| Parameter SI-4(g)-2: ISSO, System Manager | |
| Parameter SI-4(g)-3: as needed | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Security Analysts monitor the information system to achieve the following GDIT Cloud-defined monitoring objectives: 1) ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; 2) examine system records to confirm that the system is functioning in an optimal, resilient, and secure state; and 3) identify irregularities or anomalies that are indicators of a system malfunction or compromise.Security Engineers have configured system components to send logging data to the GDIT Cloud SIEM solution. See AU-2 part d for details on what system components send logging data and the type of logging data that is sent. The SIEM automatically and in real-time analyzes the log data that it receives and uses over 3,500 correlation rules to detect suspicious activities in the system. Correlation rules define a condition to match incoming events. Event correlation enables Security Analysts to: make informed decisions on how to respond to security threats; validate effectiveness of existing security controls; measure and report compliance; and detect policy violations. The SIEM helps GDIT Cloud to achieve its security monitoring objectives as follows: Ensure the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements The SIEM’s correlation rules look for system errors and anomalies that could indicate control failures. Examine system records to confirm that the system is functioning in an optimal, resilient, and secure state The SIEM receives system records from all system components and provides alerting (per the correlation rules) in situations indicating denial of service attacks or other attacks that could compromise system security and resiliency. Identify irregularities or anomalies that are indicators of a system malfunction or compromise Correlation rules provide the capability of detecting situations that could indicate a system malfunction or compromise. The SIEM has been configured to implement the above listed monitoring objectives and send alerts to the the Security Analysts and to Cherwell to open an incident ticket to initiate investigation into the events. The SIEM enables the detection of unauthorized connections whether they are local, network, or remote connections through the use of correlation events created to look for brute force attacks, and other types of connections such as SSH and telnet. |
| Part b | Security Analysts identify unauthorized use of the information system through the following techniques and methods: The GDIT Cloud MMS platforms are configured to look at the incoming log and trap stream and perform correlation on words, phrases, event codes and raise notifications to the GDIT Cloud Ticketing system where Security Analysts review the alert to determine if it is malicious. The GDIT Cloud MMS SIEM monitors all devices in the environment and conducts automatic, real-time correlation of events that are sent to the SIEM solution from the various components. If someone attempts to enter or execute a command or go to a location not authorized the correlation rules feed into the correlation directives which trip an alarm. |
| Part c | Security Engineers have deployed monitoring devices: Strategically within the information system to collect organization-determined essential information Security Engineers have deployed the Cisco Intrusion Detection System (IDS) that protects all GDIT Cloud systems. The IDS system monitors all internet traffic to/from the IaaS. The IDS sends event logs, including alerts, to the SIEM solution to be incorporated in the event correlation. See part a of this control for more details on event correlation rules. At ad hoc locations within the system to track specific types of transactions of interest to the organization All devices in the system are configured to either have an OSSEC agent to push log events to the SIEM solution or are configured to push syslog and other events to the SIEM solution. This essentially creates a whole-system monitoring configuration as follows: GDIT Cloud maintains the Cisco Intrusion Detection System (IDS) that protects all GDIT Cloud systems. The IDS system monitors all Internet communication to/from the IaaS and alerts Security Analysts to any events that might pose a threat. The GDIT Cloud MMS host-based protection is installed on all GDIT Cloud systems in the GDIT Cloud to provide assurance that nothing is being changed without informing Security Analysts. |
| Part d | GDIT Cloud protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion as follows: Access to the SIEM solution and the logging data therein is restricted and is governed by the processes described in AC-2 parts d,e, and f and enforced by the process described in AC-3. The Security Engineers have configured the SIEM solution to automatically hash log records in the system as they are received. If a log record is modified, the modified record will not match the original hash and will be identified and flagged by the SIEM solution as invalid. All devices send logging data to the GDIT Cloud SIEM solution. In the event that a user (authorized or unauthorized) successfully clears or deletes log data from a specific device (such as a server), the log data is not lost. The log data pushed out to the SIEM solution is preserved outside of the original device. |
| Part e | Security Analysts heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information, as follows: Security Analysts monitor the global and local security situation by subscribing to and monitoring various mailing lists (i.e., US-CERT) and websites (See SI-2 part a) to keep informed of the global threat and vulnerability status. In the event an alert is transmitted, Security Analysts determine if the threat or vulnerability has a potential of impacting GDIT Cloud. If the alert indicates a possible impact to GDIT Cloud, Security Analysts can engage in or initiate one or all of the following measures to heighten the level of information system monitoring activity: Conduct an ad-hoc meeting to discuss the implications of the threat/vulnerability data and what should be done to mitigate any potential risk; Reach out to tenants if necessary to share threat data and communicate any other details needed to heighten monitoring; Update the use cases (correlation events) in the GDIT Cloud MMS SIEM AlienVault to increase its detection capability; Ensure that host-based detection capabilities (i.e., Symantec and Tripwire), are at the latest update available\*; Ensure that signatures in the IDSs have been updated\*; Review specific logging activity pertinent to the threat or vulnerability data; Add or modify firewall rules to address the level of increased threat. For example, if a threat indicator contains a specific IP address, the firewall rules can be modified to ensure that traffic from that address is blocked. \*Note: Signatures are updated frequently; however, these steps are conducted to ensure the latest signatures have been applied and they are working properly (e.g., no errors or problems detected with the update(s)). |
| Part f | The ISSO obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. GDIT Cloud has at its disposal the GDIT Legal Department, which comprises several teams, including an Assistant General Counsel assigned to the HCSD organization. GDIT legal and HR teams are consulted where monitoring may impact privacy laws and or confidentiality of data. Proactively, this consultation is most prominent in “Consent to Monitoring” language presented on login banners presented upon authentication as covered in control AC-8 System Use Notification, as well as general understanding and acknowledgment of user activity monitoring outlined in PL-4 Rules of Behavior (ROB). Customer Responsibility Customers are responsible for obtaining legal opinion with regard to information system monitoring activities on their systems, regardless of who is conducting the monitoring. |
| Part g | Security Engineers configure the SIEM to provide monitoring information to the ISSO and System Manager, as needed. |

### SI-5 Security Alerts & Advisories (L) (M) (H)

The organization:

1. Receives information system security alerts, advisories, and directives from [FedRAMP Assignment: to include US-CERT] on an ongoing basis;
2. Generates internal security alerts, advisories, and directives as deemed necessary;
3. Disseminates security alerts, advisories, and directives to [FedRAMP Assignment: to include system security personnel and administrators with configuration/patch-management responsibilities]; and
4. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

| SI-5 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analysts | |
| Parameter SI-5(a): to include US-CERT | |
| Parameter SI-5(c): to include system security personnel and administrators with configuration/patch-management responsibilities | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. ,Date of Authorization | |

| SI-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud ISSO receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis. For instance, the GDIT Cloud ISSO subscribes to US CERT email alerts in order to receive timely information regarding threats, vulnerabilities, and other security-related information. In addition, the FedRAMP ISSO sends questions and alerts to the GDIT Cloud ISSO and asks for specific information. |
| Part b | Security analysts are tasked with generating internal security alerts, advisories, and directives and notifying appropriate GDIT Cloud Operations personnel in the case of security related events. The notification occurs through a GDIT Cloud Ticketing system (Cherwell) to the GDIT Cloud Operations team and references the details of the situation discovered. |
| Part c | Security analysts disseminate security alerts, advisories, and directives to appropriate GDIT Cloud Operations personnel as referenced in the table below. The notification occurs through a GDIT Cloud ticketing system (Cherwell) to the GDIT Cloud Operations team and references the details of the situation discovered. |
| Part d | GDIT Cloud implements security directives provided by the FedRAMP ISSO in accordance with established time frames specific to each directive. The GDIT Cloud ISSO opens a Cherwell ticket in order to gather the required information or begin implementation of directive change. For instance, if a directive came from the FedRAMP ISSO with the established timeframe of 24 hours response time, then the GDIT Cloud ISSO or designee would open a Cherwell ticket with a ‘Priority 1 Impact - Production Critical’ priority. The ticket would include either a request for change or request for information. Ultimately, the GDIT Cloud ISSO would respond within the timeframe to the FedRAMP ISSO with updates on actions taken and/or the degree of noncompliance, if applicable. The expected time to respond to the ‘Priority 1 Impact - Production Critical’ priority incident is as follows: |

### SI-12 Information Output Handling and Retention (L) (M) (H)

The organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

| SI-12 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization | |

| SI-12 What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud does not have physical outputs that need handling or retention considerations. Output handling is Information to Customers (email with vulnerability reports) CAB communication GDIT personnel through email Internal Information Handled through communications of all systems to our SIEM (e.g. AlienVault). Store and retain information for 12 months The GDIT Cloud does not have printers that precludes handling instructions Emails: contained solely in the email system and retained for 12 months Retention policy - records are stored within the GDIT Cloud MMS SIEM and retained for 12 months in accordance with applicable Federal laws and Requirements. The GDIT Cloud does not use devices such as printers and backups tapes as part of the system architecture. Audit data |

### SI-16 Memory Protection (L) (M) (H)

The information system implements [Assignment: organization-defined fail-safe procedures] to protect its memory from unauthorized code execution.

| SI-16 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter SI-16-1: VMware memory isolation | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  Service Provider Corporate  Service Provider System Specific  Service Provider Hybrid (Corporate and System Specific)  Configured by Customer (Customer System Specific)  Provided by Customer (Customer System Specific)  Shared (Service Provider and Customer Responsibility)  Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of AuthorizationDate of Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| The System Administrators implement VMware memory isolation to protect its memory from unauthorized code execution. Secure isolation of virtual machines occurs at the virtualization layer. This includes secure memory isolation. Memory pages that are identical in two or more virtual machines are stored once in the host system’s RAM, and each of the virtual machines has read-only access. Such shared pages are common, for example, if many virtual machines on the same host run the same OS. As soon as any one virtual machine attempts to modify a shared page, it gets its own private copy. Because shared memory pages are marked copy-on-write, it is impossible for one virtual machine to leak private information to another through this mechanism. Transparent page sharing is controlled by the VMkernel and VMM and cannot be compromised by virtual machines. It can also be disabled on a per-host or per–virtual machine basis. Each virtual machine is isolated from other virtual machines running on the same hardware. Virtual machines share physical resources such as CPU, memory, and I/O devices; a guest OS in an individual virtual machine cannot detect any device other than the virtual devices made available to it. A virtual machine cannot map to a device that has not been preassigned. A virtual machine is incapable of mounting another virtual machine’s disk unless the disk has been explicitly assigned to both virtual machines in the management console; for example, VMware vCenter™ or ESXi. |

# Acronyms

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/documents) page.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.

# Systems Security Plan Attachments

Instruction: Attach any documents that are referred to in the GDIT Cloud IaaS (GDIT Cloud) System Security Plan. Documents and attachments should, provide the title, version and exact file name, including the file extension. All attachments and associated documents must be delivered separately. No embedded documents will be accepted.

Delete this and all other instructions from your final version of this document.

# Attachments

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

* The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15‑1. to differentiate between them using the “xx” portion of the File Name. Example GDIT Cloud A1 ISPP xx v1.0. Delete the “xx” if there is only one document.
* Enter the file extension for each attachment.
* Do not change the Version Number in the File Name in Table 15‑1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15‑1. Names of Provided Attachments

| Attachment | File Name | File Extension |
| --- | --- | --- |
| Information Security Policies and Procedures | GDIT Cloud A1 ISPP xx v1.0 | . enter extension |
| User Guide | GDIT Cloud A2 UG v1.0 | . enter extension |
| Digital Identity Worksheet | Included in Section 15 |  |
| PTA | Included in Section 15 |  |
| PIA If needed) | GDIT Cloud A4 PIA v1.0 | . enter extension |
| Rules of Behavior | GDIT Cloud A5 ROB v1.0 | . enter extension |
| Information System Contingency Plan | GDIT Cloud A6 ISCP v1.0 | . enter extension |
| Configuration Management Plan | GDIT Cloud A7 CMP v1.0 | . enter extension |
| Incident Response Plan | GDIT Cloud A8 IRP v1.0 | . enter extension |
| CIS Workbook | GDIT Cloud A9 CIS Workbook v1.0 | . enter extension |
| FIPS 199 | Included in Section 15 |  |
| Inventory | GDIT Cloud A13 INV v1.0 | . enter extension |

1. Information Security Policies and Procedures

All Authorization Packages must include an Information Security Policies and Procedures attachment, which will be reviewed for quality.

1. User Guide

All Authorization Packages must include a User Guide attachment, which will be reviewed for quality.

1. Digital Identity Worksheet

This Attachment Section has been revised to include the Digital Identity template. Therefore, a separate attachment is not needed. Delete this note and all other instructions from your final version of this document.

The Digital Identity section explains the objective for selecting the appropriate Digital Identity levels for the candidate system. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63, Revision 3, Digital Identity Guidelines.

### Introduction and Purpose

This document provides guidance on digital identity services (Digital Identity, which is the process of establishing confidence in user identities electronically presented to an information system). Authentication focuses on the identity proofing process (IAL), the authentication process (AAL), and the assertion protocol used in a federated environment to communicate authentication and attribute information (if applicable) (FAL). NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Level of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

NIST SP 800-63-3 can be found at the following URL: [NIST SP 800-63-3](https://pages.nist.gov/800-63-3/)

### Information System Name/Title

This Digital Identity Plan provides an overview of the security requirements for the GDIT Cloud IaaS (GDIT Cloud) in accordance with NIST SP 800-63-3.

Table 15‑2. Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| F1303191948 | GDIT Cloud IaaS | GDIT Cloud |

### Digital Identity Level Definitions

NIST SP 800-63-3 defines three levels in each of the components of identity assurance to categorize a federal information system’s Digital Identity posture. NIST SP 800-63-3 defines the Digital Identity levels as:

* IAL – refers to the identity proofing process.
* AAL – refers to the authentication process.
* FAL – refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable) to a relying party (RP).

FedRAMP maps its system categorization levels to NIST 800-63-3’s levels as shown in Table 15-3:

Table 15‑3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels

| FedRAMP System Categorization | Identity Assurance Level (IAL) | Authenticator Assurance Level (AAL) | Federation Assurance Level (FAL) |
| --- | --- | --- | --- |
| **High** | IAL3: In-person, or supervised remote identity proofing | AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques | FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Moderate** | IAL2: In-person or remote, potentially involving a “trusted referee” | AAL2: Multi-factor required, using approved cryptographic techniques | FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it |
| **Low** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor | FAL1: Assertion is digitally signed by the identity provider |
| **FedRAMP Tailored LI-SaaS** | IAL1: Self-asserted | AAL1: Single-factor or multi-factor | FAL1: Assertion is digitally signed by the identity provider |

Selecting the appropriate Digital Identity level for a system enables the system owner to determine the right system authentication technology solution for the selected Digital Identity levels. Guidance on selecting the system authentication technology solution is available in NIST SP 800-63-3.

### Review Maximum Potential Impact Levels

PITG has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user’s asserted identity. PITG has taken into consideration the potential for harm (impact) and the likelihood of the occurrence of the harm and has identified an impact profile as found in Table 15‑4. Potential Impacts for Assurance Levels.

Assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Table 15‑4. Potential Impacts for Assurance Levels

|  | Assurance Level Impact Profile | | |
| --- | --- | --- | --- |
| Potential Impact Categories | 1 | 2 | 3 |
| Inconvenience, distress or damage to standing or reputation | Low | Mod | High |
| Financial loss or agency liability | Low | Mod | High |
| Harm to agency programs or public interests | N/A | Low/Mod | High |
| Unauthorized release of sensitive information | N/A | Low/Mod | High |
| Personal Safety | N/A | Low | Mod/High |
| Civil or criminal violations | N/A | Low/Mod | High |

### Digital Identity Level Selection

Instruction: Select the lowest level that will cover all potential impact identified from Table 15‑4. Potential Impacts for Assurance Levels.

Delete this instruction from your final version of this document.

The PITG has identified that they support the Digital Identity Level that has been selected for the Information System Name as noted in Table 15‑5. Digital Identity Level. The selected Digital Identity Level indicated is supported for federal agency consumers of the cloud service offering. Implementation details of the Digital Identity mechanisms are provided in the System Security Plan under control IA-2.

Table 15‑5. Digital Identity Level

| Digital Identity Level | Maximum Impact Profile | Selection |
| --- | --- | --- |
| Level 1: AAL1, IAL1, FAL1 | Low |  |
| Level 2: AAL2, IAL2, FAL2 | Moderate |  |
| Level 3: AAL3, IAL3, FAL3 | High |  |

1. PTA / PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in Attachment 12, FedRAMP Laws and Regulations.

### Privacy Overview and Point of Contact (POC)

The Table 15‑6. Information System Name Privacy POC individual is identified as the Information System Name Privacy Officer and POC for privacy at PITG.

Table 15‑6. Information System Name Privacy POC

| Name | Peter Harroun |
| --- | --- |
| Title | Privacy Official's Point of Contact |
| CSP / Organization | Pendeme Information Technology Group |
| Address | 11400 Westmoor Circle Suite 1014 Westminster Quebec 80021 Canada |
| Phone Number | 303-542-8492 |
| Email Address | Matthew.Holcomb@GDIT.com |

#### Applicable Laws and Regulations

The FedRAMP Laws and Regulations may be found on: [Templates](https://www.fedramp.gov/templates). A summary of FedRAMP Laws and Regulations is included in the System Security Plan (SSP) Attachment 12, FedRAMP Laws and Regulations.

Table 12‑1. GDIT Cloud IaaS Laws and Regulations include additional laws and regulations that are specific to GDIT Cloud IaaS. These will include laws and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 15‑7. GDIT Cloud IaaS Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### Applicable Standards and Guidance

The FedRAMP Standards and Guidance may be found on: [Templates](https://www.fedramp.gov/templates). The FedRAMP Standards and Guidance is included in the System Security Plan (SSP) ATTACHMENT 12 – FedRAMP Laws and Regulations. For more information, see the FedRAMP website.

Table 12‑2. GDIT Cloud IaaS Standards and Guidance includes any additional standards and guidance that are specific to GDIT Cloud IaaS. These will include standards and guidance from Federal Information Processing Standard (FIPS) and National Institute of Standards and Technology (NIST) Special Publications (SP).

Table 15‑8. GDIT Cloud IaaS Standards and Guidance

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Click here to enter text. | Click here to enter text. | Click here to enter text. |

#### Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

* Social Security numbers
* Passport numbers
* Driver’s license numbers
* Biometric information
* DNA information
* Bank account numbers

PII does not refer to business information or government information that cannot be traced back to an individual person.

### Privacy Threshold Analysis

PITG performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the GDIT Cloud IaaS (GDIT Cloud) components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by PITG can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| Select One | Does the ISA collect, maintain, or share PII in any identifiable form? |
| Select One | Does the ISA collect, maintain, or share PII information from or about the public? |
| Select One | Has a Privacy Impact Assessment ever been performed for the ISA? |
| Select One | Is there a Privacy Act System of Records Notice (SORN) for this ISA system?  If yes; the SORN identifier and name is: Enter SORN ID/Name. |

If answers to Questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are “Yes” then complete a Privacy Impact Assessment.

#### Designation

Check one.

|  |  |
| --- | --- |
|  | A Privacy Sensitive System |
|  | Not a Privacy Sensitive System (in its current version) |

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

1. Rules of Behavior

All Authorization Packages must include a Rules of Behavior (RoB) attachment, which will be reviewed for quality.

The RoB describes controls associated with user responsibilities and certain expectations of behavior for following security policies, standards and procedures. Security control PL-4 requires a CSP to implement rules of behavior.

The Rules of Behavior Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

The Template provides two example sets of rules of behavior: one for Internal Users and one for External Users. The CSP should modify each of these two sets to define the rules of behavior necessary to secure their system.

1. Information System Contingency Plan

All Authorization Packages must include an Information System Contingency Plan attachment, which will be reviewed for quality.

The Information System Contingency Plan Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

The Information System Contingency Plan Template is provided for CSPs, 3PAOs, government contractors working on FedRAMP projects, government employees working on FedRAMP projects and any outside organizations that want to make use of the FedRAMP Contingency Planning process.

1. Configuration Management Plan

All Authorization Packages must include a Configuration Management Plan attachment, which will be reviewed for quality.

1. Incident Response Plan

All Authorization Packages must include an Incident Response Plan attachment, which will be reviewed for quality.

1. CIS Workbook

All Authorization Packages must include Control Implementation Summary (CIS) Workbook attachment, which will be reviewed for quality.

The Template can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

1. FIPS 199

This Attachment Section has been revised to include the FIPS 199 Template. Therefore, a separate PTA attachment is not needed. Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Federal Information Processing Standard (FIPS) 199 Section, which will be reviewed for quality.

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: IaaS, PaaS and SaaS. The ultimate goal of the security categorization is for the CSP to be able to select and implement the FedRAMP security controls applicable to its environment.

### Introduction and Purpose

This section is intended to be used by service providers who are applying for an Authorization through the U.S. federal government FedRAMP program.

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 FIPS199 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.

The purpose of the FIPS199 Categorization report 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 report will aid the CSP in selection and implementation of FedRAMP security controls at the determined categorization level.

### Scope

The scope of the FIPS199 Categorization report includes the assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume II Revision 1 Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories.

### System Description

The GDIT Cloud IaaS system has been determined to have a security categorization of Choose level.

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).   
Delete this instruction from your final version of this document.

### 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, the CSP should also consult Appendix D.2. After reviewing the NIST guidance on Information Types, the CSP should fill out Table 15‑9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1.   
Delete this instruction from your final version of this document.

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 PUB 199 is the high watermark for the impact level of all the applicable information types.

The FIPS PUB 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 Categorization report analysis for their own data hosted on the CSP’s cloud environment. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

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.   
Delete this instruction from your final version of this document.

The Table 15‑9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1below uses the NIST SP 800-60 V2 R1 Volume II Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories to identify information types with the security impacts.

Table 15‑9. 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 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Contingency Planning | fips-199-moderate | fips-199-moderate | fips-199-moderate | fips-199-moderate | fips-199-moderate | fips-199-moderate | Click or tap here to enter text. |
| Continuity of Operations | fips-199-moderate | fips-199-moderate | fips-199-moderate | fips-199-moderate | fips-199-moderate | fips-199-moderate | Click or tap here to enter text. |
| Service Recovery | fips-199-low | fips-199-moderate | fips-199-low | fips-199-low | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| Help Desk Services | fips-199-low | fips-199-low | fips-199-low | fips-199-low | fips-199-low | fips-199-low | Click or tap here to enter text. |
| Security Management | fips-199-moderate | fips-199-moderate | fips-199-low | fips-199-moderate | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| Lifestyle/Change Management | fips-199-low | fips-199-moderate | fips-199-low | fips-199-low | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| System Maintenance | fips-199-low | fips-199-moderate | fips-199-low | fips-199-low | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| IT Infrastructure Maintenance | fips-199-low | fips-199-low | fips-199-low | fips-199-low | fips-199-low | fips-199-low | Click or tap here to enter text. |
| Information Security | fips-199-low | fips-199-moderate | fips-199-low | fips-199-low | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| System & Network Monitoring | fips-199-moderate | fips-199-moderate | fips-199-low | fips-199-moderate | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| A Privacy Sensitive System | fips-199-moderate | fips-199-moderate | fips-199-low | fips-199-moderate | fips-199-moderate | fips-199-low | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |
| Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. | Click or tap here to enter text. |

1. Separation of Duties Matrix

All Authorization Packages have the option to provide a Separation of Duties Matrix attachment, which will be reviewed for quality.

Attachment 11, Separation of Duties Matrix is referenced in the following control:

AC-5 Separation of Duties Additional FedRAMP Requirements and Guidance

1. FedRAMP Laws and Regulations

The Table 15‑10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance lists all of the FedRAMP templates in which FedRAMP laws, regulations, standards and guidance are referenced.

Table 15‑10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance

| Phase | | Document Title | |
| --- | --- | --- | --- |
| Document Phase | | SSP | System Security Plan |
|  | SSP Attachment 4 | PTA/PIA | Privacy Threshold Analysis and Privacy Impact Assessment |
|  | SSP Attachment 6 | ISCP | Information System Contingency Plan |
|  | SSP Attachment 10 | FIPS 199 | FIPS 199 Categorization |
| Assess Phase | | SAP | Security Assessment Plan |
| Authorize Phase | | SAR | Security Assessment Report |

The FedRAMP Laws and Regulations can be submitted as an appendix or an attachment. The attachment can be found on this page: [Templates](https://www.fedramp.gov/templates).

Note: All NIST Computer Security Publications can be found at the following  
URL: <http://csrc.nist.gov/publications/PubsSPs.html>

1. FedRAMP Inventory Workbook

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

* System Security Plan
* Security Assessment Plan
* Security Assessment Report
* Information System Contingency Plan
* Initial POAM
* Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: [Templates](https://www.fedramp.gov/templates).

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.