|  |
| --- |
| General Dynamics Information Technology (GDIT) Cloud IaaS System Security Plan (SSP) Moderate Baseline    General Dynamics Information Technology  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 | General Dynamics Information Technology |
| Street Address | 3060 Williams Drive |
| Suite/Room/Building | Suite 100 |
| City, State Zip | Fairfax VA 22031 us |

Prepared for

|  |  |  |
| --- | --- | --- |
| **Identification of Cloud Service Provider** | | |
|  | Organization Name | General Dynamics Information Technology |
| Street Address | 3060 Williams Drive |
| Suite/Room/Building | Suite 100 |
| City, State Zip | Fairfax VA 22031 us |

Template Revision History

|  |  |
| --- | --- |
| **Date** | **Description** |
| 6/20/2016 | 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 Section 10 and Attachment 13  Removed chapter numbers from Attachments  Removed 3 questions from Sec 2.3 E-Authentication Determination |
| 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 | Author |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <Revision Description> | <Version> | <Author> |
| <Date> | <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](#_Toc522288936)

[2. Information System Categorization 1](#_Toc522288937)

[2.1. Information Types 1](#_Toc522288938)

[2.2. Security Objectives Categorization (FIPS 199) 3](#_Toc522288939)

[2.3. Digital Identity Determination 3](#_Toc522288940)

[3. Information System Owner 4](#_Toc522288941)

[4. Authorizing Officials 4](#_Toc522288942)

[5. Other Designated Contacts 4](#_Toc522288943)

[6. Assignment of Security Responsibility 5](#_Toc522288944)

[7. Information System Operational Status 6](#_Toc522288945)

[8. Information System Type 7](#_Toc522288946)

[8.1. Cloud Service Models 7](#_Toc522288947)

[8.2. Cloud Deployment Models 8](#_Toc522288948)

[8.3. Leveraged Authorizations 8](#_Toc522288949)

[9. General System Description 9](#_Toc522288950)

[9.1. System Function or Purpose 9](#_Toc522288951)

[9.2. Information System Components and Boundaries 9](#_Toc522288952)

[9.3. Types of Users 10](#_Toc522288953)

[9.4. Network Architecture 11](#_Toc522288954)

[10. System Environment and Inventory 12](#_Toc522288955)

[10.1. Data Flow 12](#_Toc522288956)

[10.2. Ports, Protocols and Services 14](#_Toc522288957)

[11. System Interconnections 15](#_Toc522288958)

[12. Laws, Regulations, Standards and Guidance 17](#_Toc522288959)

[12.1. Applicable Laws and Regulations 17](#_Toc522288960)

[12.2. Applicable Standards and Guidance 17](#_Toc522288961)

[13. Minimum Security Controls 18](#_Toc522288962)

[13.1. Access Control (AC) 25](#_Toc522288963)

[AC-1 Access Control Policy and Procedures Requirements (H) 25](#_Toc522288964)

[AC-2 Account Management (H) 26](#_Toc522288965)

[AC-2 (1) Control Enhancement (M) (H) 27](#_Toc522288966)

[AC-2 (2) Control Enhancement (H) 28](#_Toc522288967)

[AC-2 (3) Control Enhancement (H) 29](#_Toc522288968)

[AC-2 (4) Control Enhancement (H) 30](#_Toc522288969)

[AC-2 (5) Control Enhancement (H) 31](#_Toc522288970)

[AC-2 (7) Control Enhancement (H) 31](#_Toc522288971)

[AC-2 (9) Control Enhancement (H) 32](#_Toc522288972)

[AC-2 (10) Control Enhancement (M) (H) 33](#_Toc522288973)

[AC-2 (11) Control Enhancement (H) 34](#_Toc522288974)

[AC-2 (12) Control Enhancement (H) 35](#_Toc522288975)

[AC-2 (13) Control Enhancement (H) 36](#_Toc522288976)

[AC-3 Access Enforcement (L) (M) (H) 36](#_Toc522288977)

[AC-4 Information Flow Enforcement (M) (H) 37](#_Toc522288978)

[AC-4 (8) Control Enhancement (H) 38](#_Toc522288979)

[AC-4 (21) Control Enhancement (M) (H) 39](#_Toc522288980)

[AC-5 Separation of Duties (M) (H) 40](#_Toc522288981)

[AC-6 Least Privilege (M) (H) 41](#_Toc522288982)

[AC-6 (1) Control Enhancement (H) 41](#_Toc522288983)

[AC-6 (2) Control Enhancement (M) (H) 42](#_Toc522288984)

[AC-6 (3) Control Enhancement (H) 43](#_Toc522288985)

[AC 6 (5) Control Enhancement (M) (H) 44](#_Toc522288986)

[AC-6 (7) Control Enhancement (H) 44](#_Toc522288987)

[AC-6 (8) Control Enhancement (H) 45](#_Toc522288988)

[AC-6 (9) Control Enhancement (M) (H) 46](#_Toc522288989)

[AC-6 (10) Control Enhancement (M) (H) 47](#_Toc522288990)

[AC-7 Unsuccessful Login Attempts (H) 47](#_Toc522288991)

[AC-7 (2) Control Enhancement (H) 48](#_Toc522288992)

[AC-8 System Use Notification (L) (M) (H) 49](#_Toc522288993)

[AC-10 Concurrent Session Control (M) (H) 52](#_Toc522288994)

[AC-11 Session Lock (M) (H) 53](#_Toc522288995)

[AC-11 (1) Control Enhancement (M) (H) 54](#_Toc522288996)

[AC-12 Session Termination (M) (H) 54](#_Toc522288997)

[AC-12 (1) Control Enhancement (H) 55](#_Toc522288998)

[AC-14 Permitted Actions without Identification or Authentication (L) (M) (H) 56](#_Toc522288999)

[AC-17 Remote Access (L) (M) (H) 57](#_Toc522289000)

[AC-17 (1) Control Enhancement (M) (H) 58](#_Toc522289001)

[AC-17 (2) Control Enhancement (M) (H) 58](#_Toc522289002)

[AC-17 (3) Control Enhancement (M) (H) 59](#_Toc522289003)

[AC-17 (4) Control Enhancement (M) (H) 60](#_Toc522289004)

[AC-17 (9) Control Enhancement (M) (H) 61](#_Toc522289005)

[AC-18 Wireless Access Restrictions (L) (M) (H) 61](#_Toc522289006)

[AC-18 (1) Control Enhancement (M) (H) 62](#_Toc522289007)

[AC-18 (3) Control Enhancement (H) 63](#_Toc522289008)

[AC-18 (4) Control Enhancement (H) 64](#_Toc522289009)

[AC-18 (5) Control Enhancement (H) 64](#_Toc522289010)

[AC-19 Access Control for Portable and Mobile Systems (L) (M) (H) 65](#_Toc522289011)

[AC-19 (5) Control Enhancement (M) (H) 66](#_Toc522289012)

[AC-20 Use of External Information Systems (L) (M) (H) 67](#_Toc522289013)

[AC-20 (1) Control Enhancement (M) (H) 68](#_Toc522289014)

[AC-20 (2) Control Enhancement (M) (H) 68](#_Toc522289015)

[AC-21 Information Sharing (M) (H) 69](#_Toc522289016)

[AC-22 Publicly Accessible Content (L) (M) (H) 70](#_Toc522289017)

[13.2. Awareness and Training (AT) 71](#_Toc522289018)

[AT-1 Security Awareness and Training Policy and Procedures (H) 71](#_Toc522289019)

[AT-2 Security Awareness (L) (M) (H) 72](#_Toc522289020)

[AT-2 (2) Control Enhancement (M) (H) 73](#_Toc522289021)

[AT-3 Role-Based Security Training (L) (M) (H) 74](#_Toc522289022)

[AT-3 (3) Control Enhancement (H) 75](#_Toc522289023)

[AT-3 (4) Control Enhancement (H) 75](#_Toc522289024)

[AT-4 Security Training Records (H) 76](#_Toc522289025)

[13.3. Audit and Accountability (AU) 77](#_Toc522289026)

[AU-1 Audit and Accountability Policy and Procedures (H) 77](#_Toc522289027)

[AU-2 Audit Events (L) (M) (H) 78](#_Toc522289028)

[AU-2 (3) Control Enhancement (M) (H) 79](#_Toc522289029)

[AU-3 Content of Audit Records (L) (M) (H) 80](#_Toc522289030)

[AU-3 (1) Control Enhancement (H) 81](#_Toc522289031)

[AU-3 (2) Control Enhancement (H) 82](#_Toc522289032)

[AU-4 Audit Storage Capacity (L) (M) (H) 83](#_Toc522289033)

[AU-5 Response to Audit Processing Failures (L) (M) (H) 83](#_Toc522289034)

[AU-5 (1) Control Enhancement (H) 84](#_Toc522289035)

[AU-5 (2) Control Enhancement (H) 85](#_Toc522289036)

[AU-6 Audit Review, Analysis, and Reporting (L) (M) (H) 86](#_Toc522289037)

[AU-6 (1) Control Enhancement (M) (H) 87](#_Toc522289038)

[AU-6 (3) Control Enhancement (M) (H) 88](#_Toc522289039)

[AU-6 (4) Control Enhancement (H) 88](#_Toc522289040)

[AU-6 (5) Control Enhancement (H) 89](#_Toc522289041)

[AU-6 (6) Control Enhancement (H) 90](#_Toc522289042)

[AU-6 (7) Control Enhancement (H) 91](#_Toc522289043)

[AU-6 (10) Control Enhancement (H) 91](#_Toc522289044)

[AU-7 Audit Reduction and Report Generation (M) (H) 92](#_Toc522289045)

[AU-7 (1) Control Enhancement (M) (H) 93](#_Toc522289046)

[AU-8 Time Stamps (L) (M) (H) 94](#_Toc522289047)

[AU-8 (1) Control Enhancement (M) (H) 94](#_Toc522289048)

[AU-9 Protection of Audit Information (L) (M) (H) 96](#_Toc522289049)

[AU-9 (2) Control Enhancement (M) (H) 96](#_Toc522289050)

[AU-9 (3) Control Enhancement (H) 97](#_Toc522289051)

[AU-9 (4) Control Enhancement (M) (H) 98](#_Toc522289052)

[AU-10 Non-repudiation (H) 98](#_Toc522289053)

[AU-11 Audit Record Retention (H) 99](#_Toc522289054)

[AU-12 Audit Generation (L) (M) (H) 100](#_Toc522289055)

[AU-12 (1) Control Enhancement (H) 101](#_Toc522289056)

[AU-12 (3) Control Enhancement (H) 102](#_Toc522289057)

[13.4. Security Assessment and Authorization (CA) 103](#_Toc522289058)

[CA-1 Certification, Authorization, Security Assessment Policy and Procedures (H) 103](#_Toc522289059)

[CA-2 Security Assessments (L) (M) (H) 104](#_Toc522289060)

[CA-2 (1) Control Enhancement (L) (M) (H) 105](#_Toc522289061)

[CA-2 (2) Control Enhancement (M) (H) 106](#_Toc522289062)

[CA-2 (3) Control Enhancement (M) (H) 107](#_Toc522289063)

[CA-3 System Interconnections (L) (M) (H) 108](#_Toc522289064)

[CA-3 (3) Control Enhancement (M) (H) 109](#_Toc522289065)

[CA-3 (5) Control Enhancement (H) 110](#_Toc522289066)

[CA-5 Plan of Action and Milestones (L) (M) (H) 111](#_Toc522289067)

[CA-6 Security Authorization (L) (M) (H) 112](#_Toc522289068)

[CA-7 Continuous Monitoring (L) (M) (H) 113](#_Toc522289069)

[CA-7 (1) Control Enhancement (M) (H) 115](#_Toc522289070)

[CA-7 (3) Control Enhancement (H) 116](#_Toc522289071)

[CA-8 Penetration Testing (M) (H) 117](#_Toc522289072)

[CA-8 (1) Control Enhancement (M) (H) 118](#_Toc522289073)

[CA-9 Internal System Connections (L) (M) (H) 118](#_Toc522289074)

[13.5. Configuration Management (CM) 119](#_Toc522289075)

[CM-1 Configuration Management Policies and Procedures (H) 119](#_Toc522289076)

[CM-2 Baseline Configuration (L) (M) (H) 120](#_Toc522289077)

[CM-2 (1) Control Enhancement (H) 121](#_Toc522289078)

[CM-2 (2) Control Enhancement (M) (H) 122](#_Toc522289079)

[CM-2 (3) Control Enhancement (H) 123](#_Toc522289080)

[CM-2 (7) Control Enhancement (M) (H) 123](#_Toc522289081)

[CM-3 Configuration Change Control (M) (H) 124](#_Toc522289082)

[CM-3 (1) Control Enhancement (H) 126](#_Toc522289083)

[CM-3 (2) Control Enhancement (M)(H) 127](#_Toc522289084)

[CM-3 (4) Enhancement (H) 128](#_Toc522289085)

[CM-3 (6) Enhancement (H) 128](#_Toc522289086)

[CM-4 Security Impact Analysis (L) (M) (H) 129](#_Toc522289087)

[CM-4 (1) Control Enhancement (H) 130](#_Toc522289088)

[CM-5 Access Restrictions for Change (M) (H) 131](#_Toc522289089)

[CM-5 (1) Control Enhancement (M) (H) 131](#_Toc522289090)

[CM-5 (2) Control Enhancement (H) 132](#_Toc522289091)

[CM-5 (3) Control Enhancement (M) (H) 133](#_Toc522289092)

[CM-5 (5) Control Enhancement (M) (H) 134](#_Toc522289093)

[CM-6 Configuration Settings (L) (M) (H) 134](#_Toc522289094)

[CM-6 (1) Control Enhancement (M) (H) 136](#_Toc522289095)

[CM-6 (2) Control Enhancement (H) 136](#_Toc522289096)

[CM-7 Least Functionality (L) (M) (H) 137](#_Toc522289097)

[CM-7 (1) Control Enhancement (M) (H) 138](#_Toc522289098)

[CM-7 (2) Control Enhancement (M) (H) 139](#_Toc522289099)

[CM-7 (5) Control Enhancement (H) 140](#_Toc522289100)

[CM-8 Information System Component Inventory (L) (M) (H) 141](#_Toc522289101)

[CM-8 (1) Control Enhancement (M) (H) 142](#_Toc522289102)

[CM-8 (2) Control Enhancement (H) 143](#_Toc522289103)

[CM-8 (3) Control Enhancement (M) (H) 144](#_Toc522289104)

[CM-8 (4) Control Enhancement (H) 145](#_Toc522289105)

[CM-8 (5) Control Enhancement (M) (H) 145](#_Toc522289106)

[CM-9 Configuration Management Plan (M) (H) 146](#_Toc522289107)

[CM-10 Software Usage Restrictions (L) (M) (H) 147](#_Toc522289108)

[CM-10 (1) Control Enhancement (M) (H) 148](#_Toc522289109)

[CM-11 User-Installed Software (M) (H) 149](#_Toc522289110)

[CM-11 (1) Control Enhancement (H) 150](#_Toc522289111)

[13.6. Contingency Planning (CP) 150](#_Toc522289112)

[CP-1 Contingency Planning Policy and Procedures (H) 150](#_Toc522289113)

[CP-2 Contingency Plan (L) (M) (H) 151](#_Toc522289114)

[CP-2 (1) Control Enhancement (M) (H) 153](#_Toc522289115)

[CP-2 (2) Control Enhancement (M) (H) 154](#_Toc522289116)

[CP-2 (3) Control Enhancement (M) (H) 154](#_Toc522289117)

[CP-2 (4) Control Enhancement (H) 155](#_Toc522289118)

[CP-2 (5) Control Enhancement (H) 156](#_Toc522289119)

[CP-2 (8) Control Enhancement (M) (H) 157](#_Toc522289120)

[CP-3 Contingency Training (L) (M) (H) 157](#_Toc522289121)

[CP-3 (1) Control Enhancement (H) 158](#_Toc522289122)

[CP-4 Contingency Plan Testing (H) 159](#_Toc522289123)

[CP-4 (1) Control Enhancement (M) (H) 160](#_Toc522289124)

[CP-4 (2) Control Enhancement (H) 161](#_Toc522289125)

[CP-6 Alternate Storage Site (M) (H) 161](#_Toc522289126)

[CP-6 (1) Control Enhancement (M) (H) 162](#_Toc522289127)

[CP-6 (2) Control Enhancement (H) 163](#_Toc522289128)

[CP-6 (3) Control Enhancement (M) (H) 164](#_Toc522289129)

[CP-7 Alternate Processing Site (M) (H) 164](#_Toc522289130)

[CP-7 (1) Control Enhancement (M) (H) 165](#_Toc522289131)

[CP-7 (2) Control Enhancement (M) (H) 166](#_Toc522289132)

[CP-7 (3) Control Enhancement (M) (H) 167](#_Toc522289133)

[CP-7 (4) Control Enhancement (H) 168](#_Toc522289134)

[CP-8 Telecommunications Services (M) (H) 168](#_Toc522289135)

[CP-8 (1) Control Enhancement (M) (H) 169](#_Toc522289136)

[CP-8 (2) Control Enhancement (M) (H) 170](#_Toc522289137)

[CP-8 (3) Control Enhancement (H) 171](#_Toc522289138)

[CP-8 (4) Control Enhancement (H) 171](#_Toc522289139)

[CP-9 Information System Backup (L) (M) (H) 172](#_Toc522289140)

[CP-9 (1) Control Enhancement (H) 174](#_Toc522289141)

[CP-9 (2) Control Enhancement (H) 174](#_Toc522289142)

[CP-9 (3) Control Enhancement (M) (H) 175](#_Toc522289143)

[CP-9 (5) Control Enhancement (H) 176](#_Toc522289144)

[CP-10 Information System Recovery and Reconstitution (L) (M) (H) 177](#_Toc522289145)

[CP-10 (2) Control Enhancement (M) (H) 177](#_Toc522289146)

[CP-10 (4) Control Enhancement (H) 178](#_Toc522289147)

[13.7. Identification and Authentication (IA) 179](#_Toc522289148)

[IA-1 Identification and Authentication Policy and Procedures (H) 179](#_Toc522289149)

[IA-2 User Identification and Authentication (L) (M) (H) 180](#_Toc522289150)

[IA-2 (1) Control Enhancement (L) (M) (H) 181](#_Toc522289151)

[IA-2 (2) Control Enhancement (M) (H) 181](#_Toc522289152)

[IA-2 (3) Control Enhancement (M) (H) 182](#_Toc522289153)

[IA-2 (4) Control Enhancement (H) 183](#_Toc522289154)

[IA-2 (5) Control Enhancement (M) (H) 183](#_Toc522289155)

[IA-2 (8) Control Enhancement (M) (H) 184](#_Toc522289156)

[IA-2 (9) Control Enhancement (H) 185](#_Toc522289157)

[IA-2 (11) Control Enhancement (M) (H) 185](#_Toc522289158)

[IA-2 (12) Control Enhancement (L) (M) (H) 186](#_Toc522289159)

[IA-3 Device Identification and Authentication (M) (H) 187](#_Toc522289160)

[IA-4 Identifier Management (H) 188](#_Toc522289161)

[IA-4 (4) Control Enhancement (M) (H) 189](#_Toc522289162)

[IA-5 Authenticator Management (H) 190](#_Toc522289163)

[IA-5 (1) Control Enhancement (H) 191](#_Toc522289164)

[IA-5 (2) Control Enhancement (M) (H) 193](#_Toc522289165)

[IA-5 (3) Control Enhancement (M) (H) 194](#_Toc522289166)

[IA-5 (4) Control Enhancement (H) 195](#_Toc522289167)

[IA-5 (6) Control Enhancement (M) (H) 195](#_Toc522289168)

[IA-5 (7) Control Enhancement (M) (H) 196](#_Toc522289169)

[IA-5 (8) Control Enhancement (H) 197](#_Toc522289170)

[IA-5 (11) Control Enhancement (L) (M) (H) 198](#_Toc522289171)

[IA-5 (13) Control Enhancement (H) 198](#_Toc522289172)

[IA-6 Authenticator Feedback (L) (M) (H) 199](#_Toc522289173)

[IA-7 Cryptographic Module Authentication (L) (M) (H) 200](#_Toc522289174)

[IA-8 Identification and Authentication (Non-Organizational Users) (L) (M) (H) 200](#_Toc522289175)

[IA-8 (1) Control Enhancement (L) (M) (H) 201](#_Toc522289176)

[IA-8 (2) Control Enhancement (L) (M) (H) 202](#_Toc522289177)

[IA-8 (3) Control Enhancement (L) (M) (H) 202](#_Toc522289178)

[IA-8 (4) Control Enhancement (L) (M) (H) 203](#_Toc522289179)

[13.8. Incident Response (IR) 204](#_Toc522289180)

[IR-1 Incident Response Policy and Procedures (H) 204](#_Toc522289181)

[IR-2 Incident Response Training (H) 205](#_Toc522289182)

[IR-2 (1) Control Enhancement (H) 206](#_Toc522289183)

[IR-2 (2) Control Enhancement (H) 207](#_Toc522289184)

[IR-3 Incident Response Testing (H) 207](#_Toc522289185)

[IR-3 (2) Control Enhancement (M) (H) 208](#_Toc522289186)

[IR-4 Incident Handling (L) (M) (H) 209](#_Toc522289187)

[IR-4 (1) Control Enhancement (M) (H) 210](#_Toc522289188)

[IR-4 (2) Control Enhancement (H) 211](#_Toc522289189)

[IR-4 (3) Control Enhancement (H) 211](#_Toc522289190)

[IR-4 (4) Control Enhancement (H) 212](#_Toc522289191)

[IR-4 (6) Control Enhancement (H) 213](#_Toc522289192)

[IR-4 (8) Control Enhancement (H) 213](#_Toc522289193)

[IR-5 Incident Monitoring (L) (M) (H) 214](#_Toc522289194)

[IR-5 (1) Control Enhancement (H) 215](#_Toc522289195)

[IR-6 Incident Reporting (L) (M) (H) 216](#_Toc522289196)

[IR-6 (1) Control Enhancement (M) (H) 217](#_Toc522289197)

[IR-7 Incident Response Assistance (L) (M) (H) 217](#_Toc522289198)

[IR-7 (1) Control Enhancement (M) (H) 218](#_Toc522289199)

[IR-7 (2) Control Enhancement (M) (H) 219](#_Toc522289200)

[IR-8 Incident Response Plan (L) (M) (H) 219](#_Toc522289201)

[IR-9 Information Spillage Response (M) (H) 221](#_Toc522289202)

[IR-9 (1) Control Enhancement (M) (H) 222](#_Toc522289203)

[IR-9 (2) Control Enhancement (H) 223](#_Toc522289204)

[IR-9 (3) Control Enhancement (M) (H) 224](#_Toc522289205)

[IR-9 (4) Control Enhancement (M) (H) 225](#_Toc522289206)

[13.9. Maintenance (MA) 225](#_Toc522289207)

[MA-1 System Maintenance Policy and Procedures (H) 225](#_Toc522289208)

[MA-2 Controlled Maintenance (L) (M) (H) 226](#_Toc522289209)

[MA-2 (2) Control Enhancement (H) 228](#_Toc522289210)

[MA-3 Maintenance Tools (M) (H) 229](#_Toc522289211)

[MA-3 (1) Control Enhancement (M) (H) 229](#_Toc522289212)

[MA-3 (2) Control Enhancement (M) (H) 230](#_Toc522289213)

[MA-3 (3) Control Enhancement (M) (H) 231](#_Toc522289214)

[MA-4 Remote Maintenance (L) (M) (H) 232](#_Toc522289215)

[MA-4 (2) Control Enhancement (M) (H) 233](#_Toc522289216)

[MA-4 (3) Control Enhancement (H) 233](#_Toc522289217)

[MA-4 (6) Enhancement (H) 234](#_Toc522289218)

[MA-5 Maintenance Personnel (L) (M) (H) 235](#_Toc522289219)

[MA-5 (1) Control Enhancement (H) 236](#_Toc522289220)

[MA-6 Timely Maintenance (M) (H) 237](#_Toc522289221)

[13.10. Media Protection (MP) 238](#_Toc522289222)

[MP-1 Media Protection Policy and Procedures (H) 238](#_Toc522289223)

[MP-2 Media Access (H) 239](#_Toc522289224)

[MP-3 Media Labeling (M) (H) 240](#_Toc522289225)

[MP-4 Media Storage (M) (H) 241](#_Toc522289226)

[MP-5 Media Transport (M) (H) 242](#_Toc522289227)

[MP-5 (4) Control Enhancement (M) (H) 243](#_Toc522289228)

[MP-6 Media Sanitization and Disposal (H) 244](#_Toc522289229)

[MP-6 (1) Control Enhancement (H) 245](#_Toc522289230)

[MP-6 (2) Control Enhancement (H) 246](#_Toc522289231)

[MP-6 (3) Control Enhancement (H) 247](#_Toc522289232)

[MP-7 Media Use (L) (M) (H) 247](#_Toc522289233)

[MP-7 (1) Control Enhancement (M) (H) 248](#_Toc522289234)

[13.11. Physical and Environmental Protection (PE) 249](#_Toc522289235)

[PE-1 Physical and Environmental Protection Policy and Procedures (H) 249](#_Toc522289236)

[PE-2 Physical Access Authorizations (H) 250](#_Toc522289237)

[PE-3 Physical Access Control (L) (M) (H) 251](#_Toc522289238)

[PE-3 (1) Control Enhancement (H) 253](#_Toc522289239)

[PE-4 Access Control for Transmission Medium (M) (H) 254](#_Toc522289240)

[PE-5 Access Control for Output Devices (M) (H) 254](#_Toc522289241)

[PE-6 Monitoring Physical Access (L) (M) (H) 255](#_Toc522289242)

[PE-6 (1) Control Enhancement (M) (H) 256](#_Toc522289243)

[PE-6 (4) Control Enhancement (H) 257](#_Toc522289244)

[PE-8 Visitor Access Records (L) (M) (H) 258](#_Toc522289245)

[PE-8 (1) Control Enhancement (H) 259](#_Toc522289246)

[PE-9 Power Equipment and Cabling (M) (H) 259](#_Toc522289247)

[PE-10 Emergency Shutoff (M) (H) 260](#_Toc522289248)

[PE-11 Emergency Power (M) (H) 261](#_Toc522289249)

[PE-11 (1) Control Enhancement (H) 262](#_Toc522289250)

[PE-12 Emergency Lighting (L) (M) (H) 263](#_Toc522289251)

[PE-13 Fire Protection (L) (M) (H) 263](#_Toc522289252)

[PE-13 (1) Control Enhancement (H) 264](#_Toc522289253)

[PE-13 (2) Control Enhancement (M) (H) 265](#_Toc522289254)

[PE-13 (3) Control Enhancement (M) (H) 266](#_Toc522289255)

[PE-14 Temperature and Humidity Controls (L) (M) (H) 267](#_Toc522289256)

[PE-14 (2) Control Enhancement (M) (H) 268](#_Toc522289257)

[PE-15 Water Damage Protection (L) (M) (H) 268](#_Toc522289258)

[PE-15 (1) Control Enhancement (H) 269](#_Toc522289259)

[PE-16 Delivery and Removal (L) (M) (H) 270](#_Toc522289260)

[PE-17 Alternate Work Site (M) (H) 271](#_Toc522289261)

[PE-18 Location of Information System Components (H) 272](#_Toc522289262)

[13.12. Planning (PL) 272](#_Toc522289263)

[PL-1 Security Planning Policy and Procedures (H) 272](#_Toc522289264)

[PL-2 System Security Plan (L) (M) (H) 273](#_Toc522289265)

[PL-2 (3) Control Enhancement (M) (H) 275](#_Toc522289266)

[PL-4 Rules of Behavior (H) 276](#_Toc522289267)

[PL-4 (1) Control Enhancement (M) (H) 277](#_Toc522289268)

[PL-8 Information Security Architecture (M) (H) 278](#_Toc522289269)

[13.13. Personnel Security (PS) 279](#_Toc522289270)

[PS-1 Personnel Security Policy and Procedures (H) 279](#_Toc522289271)

[PS-2 Position Categorization (H) 280](#_Toc522289272)

[PS-3 Personnel Screening (L) (M) (H) 281](#_Toc522289273)

[PS-3 (3) Control Enhancement (M) (H) 282](#_Toc522289274)

[PS-4 Personnel Termination (H) 283](#_Toc522289275)

[PS-4 (2) Control Enhancement (H) 284](#_Toc522289276)

[PS-5 Personnel Transfer (H) 285](#_Toc522289277)

[PS-6 Access Agreements (H) 286](#_Toc522289278)

[PS-7 Third-Party Personnel Security (H) 287](#_Toc522289279)

[PS-8 Personnel Sanctions (H) 288](#_Toc522289280)

[13.14. Risk Assessment (RA) 289](#_Toc522289281)

[RA-1 Risk Assessment Policy and Procedures (H) 289](#_Toc522289282)

[RA-2 Security Categorization (L) (M) (H) 291](#_Toc522289283)

[RA-3 Risk Assessment (H) 292](#_Toc522289284)

[RA-5 Vulnerability Scanning (L) (M) (H) 293](#_Toc522289285)

[RA-5 (1) Control Enhancement (M) (H) 295](#_Toc522289286)

[RA-5 (2) Control Enhancement (M) (H) 295](#_Toc522289287)

[RA-5 (3) Control Enhancement (M) (H) 296](#_Toc522289288)

[RA-5 (4) Control Enhancement (H) 297](#_Toc522289289)

[RA-5 (5) Control Enhancement (M) (H) 298](#_Toc522289290)

[RA-5 (6) Control Enhancement (M) (H) 298](#_Toc522289291)

[RA-5 (8) Control Enhancement (L) (M) (H) 299](#_Toc522289292)

[RA-5 (10) Control Enhancement (H) 300](#_Toc522289293)

[13.15. System and Services Acquisition (SA) 301](#_Toc522289294)

[SA-1 System and Services Acquisition Policy and Procedures (H) 301](#_Toc522289295)

[SA-2 Allocation of Resources (L) (M) (H) 302](#_Toc522289296)

[SA-3 System Development Life Cycle (L) (M) (H) 303](#_Toc522289297)

[SA-4 Acquisitions Process (L) (M) (H) 304](#_Toc522289298)

[SA-4 (1) Control Enhancement (M) (H) 305](#_Toc522289299)

[SA-4 (2) Control Enhancement (H) 306](#_Toc522289300)

[SA-4 (8) Control Enhancement (M) (H) 307](#_Toc522289301)

[SA-4 (9) Control Enhancement (M) (H) 308](#_Toc522289302)

[SA-4 (10) Control Enhancement (M) (H) 309](#_Toc522289303)

[SA-5 Information System Documentation (H) 309](#_Toc522289304)

[SA-8 Security Engineering Principles (M) (H) 311](#_Toc522289305)

[SA-9 External Information System Services (L) (M) (H) 312](#_Toc522289306)

[SA-9 (1) Control Enhancement (M) (H) 313](#_Toc522289307)

[SA-9 (2) Control Enhancement (M) (H) 314](#_Toc522289308)

[SA-9 (4) Control Enhancement (M) (H) 314](#_Toc522289309)

[SA-9 (5) Control Enhancement (M) (H) 315](#_Toc522289310)

[SA-10 Developer Configuration Management (M) (H) 316](#_Toc522289311)

[SA-10 (1) Control Enhancement (M) (H) 317](#_Toc522289312)

[SA-11 Developer Security Testing and Evaluation (M) (H) 318](#_Toc522289313)

[SA-11 (1) Control Enhancement (M) (H) 319](#_Toc522289314)

[SA-11 (2) Control Enhancement (M) (H) 320](#_Toc522289315)

[SA-11 (8) Control Enhancement (M) (H) 321](#_Toc522289316)

[SA-12 Supply Chain Protection (H) 322](#_Toc522289317)

[SA-15 Development Process, Standards, and Tools (H) 322](#_Toc522289318)

[SA-16 Developer-Provided Training (H) 324](#_Toc522289319)

[SA-17 Developer Security Architecture and Design (H) 324](#_Toc522289320)

[13.16. System and Communications Protection (SC) 325](#_Toc522289321)

[SC-1 System and Communications Protection Policy and Procedures (H) 325](#_Toc522289322)

[SC-2 Application Partitioning (M) (H) 326](#_Toc522289323)

[SC-3 Security Function Isolation (H) 327](#_Toc522289324)

[SC-4 Information in Shared Resources (M) (H) 328](#_Toc522289325)

[SC-5 Denial of Service Protection (L) (M) (H) 329](#_Toc522289326)

[SC-6 Resource Availability (M) (H) 329](#_Toc522289327)

[SC-7 Boundary Protection (L) (M) (H) 330](#_Toc522289328)

[SC-7 (3) Control Enhancement (M) (H) 331](#_Toc522289329)

[SC-7 (4) Control Enhancement (H) 332](#_Toc522289330)

[SC-7 (5) Control Enhancement (M) (H) 333](#_Toc522289331)

[SC-7 (7) Control Enhancement (M) (H) 334](#_Toc522289332)

[SC-7 (8) Control Enhancement (M) (H) 335](#_Toc522289333)

[SC-7 (10) Control Enhancement (H) 335](#_Toc522289334)

[SC-7 (12) Control Enhancement (H) 336](#_Toc522289335)

[SC-7 (13) Control Enhancement (H) 337](#_Toc522289336)

[SC-7 (18) Control Enhancement (M) (H) 338](#_Toc522289337)

[SC-7 (20) Control Enhancement (H) 339](#_Toc522289338)

[SC-7 (21) Control Enhancement (H) 339](#_Toc522289339)

[SC-8 Transmission confidentiality and Integrity (M) (H) 340](#_Toc522289340)

[SC-8 (1) Control Enhancement (M) (H) 341](#_Toc522289341)

[SC-10 Network Disconnect (H) 342](#_Toc522289342)

[SC-12 Cryptographic Key Establishment & Management (L) (M) (H) 343](#_Toc522289343)

[SC-12 (1) Control Enhancement (H) 344](#_Toc522289344)

[SC-12 (2) Control Enhancement (M) (H) 344](#_Toc522289345)

[SC-12 (3) Control Enhancement (M) (H) 345](#_Toc522289346)

[SC-13 Use of Cryptography (L) (M) (H) 346](#_Toc522289347)

[SC-15 Collaborative Computing Devices (M) (H) 347](#_Toc522289348)

[SC-17 Public Key Infrastructure Certificates (M) (H) 348](#_Toc522289349)

[SC-18 Mobile Code (M) (H) 349](#_Toc522289350)

[SC-19 Voice Over Internet Protocol (M) (H) 350](#_Toc522289351)

[SC-20 Secure Name / Address Resolution Service (Authoritative Source) (L) (M) (H) 351](#_Toc522289352)

[SC-21 Secure Name / Address Resolution Service (Recursive or Caching Resolver) (L) (M) (H) 352](#_Toc522289353)

[SC-22 Architecture and Provisioning for Name / Address Resolution Service (L) (M) (H) 353](#_Toc522289354)

[SC-23 Session Authenticity (M) (H) 353](#_Toc522289355)

[SC-23 (1) Enhancement (H) 354](#_Toc522289356)

[SC-24 Fail in Known State (H) 355](#_Toc522289357)

[SC-28 Protection of Information at Rest (M) (H) 356](#_Toc522289358)

[SC-28 (1) Control Enhancement (H) 357](#_Toc522289359)

[SC-39 Process Isolation (L) (M) (H) 357](#_Toc522289360)

[13.17. System and Information Integrity (SI) 358](#_Toc522289361)

[SI-1 System and Information Integrity Policy and Procedures (H) 358](#_Toc522289362)

[SI-2 Flaw Remediation (L) (M) (H) 359](#_Toc522289363)

[SI-2 (1) Control Enhancement (H) 360](#_Toc522289364)

[SI-2 (2) Control Enhancement (M) (H) 361](#_Toc522289365)

[SI-2 (3) Control Enhancement (M) (H) 362](#_Toc522289366)

[SI-3 Malicious Code Protection (H) 363](#_Toc522289367)

[SI-3 (1) Control Enhancement (M) (H) 364](#_Toc522289368)

[SI-3 (2) Control Enhancement (M) (H) 365](#_Toc522289369)

[SI-3 (7) Control Enhancement (M) (H) 365](#_Toc522289370)

[SI-4 Information System Monitoring (L) (M) (H) 366](#_Toc522289371)

[SI-4 (1) Control Enhancement (M) (H) 368](#_Toc522289372)

[SI-4 (2) Control Enhancement (M) (H) 368](#_Toc522289373)

[SI-4 (4) Control Enhancement (M) (H) 369](#_Toc522289374)

[SI-4 (5) Control Enhancement (M) (H) 370](#_Toc522289375)

[SI-4 (11) Control Enhancement (H) 371](#_Toc522289376)

[SI-4 (14) Control Enhancement (M) (H) 372](#_Toc522289377)

[SI-4 (16) Control Enhancement (M) (H) 372](#_Toc522289378)

[SI-4 (18) Control Enhancement (H) 373](#_Toc522289379)

[SI-4 (19) Control Enhancement (H) 374](#_Toc522289380)

[SI-4 (20) Control Enhancement (H) 375](#_Toc522289381)

[SI-4 (22) Control Enhancement (H) 375](#_Toc522289382)

[SI-4 (23) Control Enhancement (M) (H) 376](#_Toc522289383)

[SI-4 (24) Control Enhancement (H) 377](#_Toc522289384)

[SI-5 Security Alerts & Advisories (L) (M) (H) 378](#_Toc522289385)

[SI-5 (1) Control Enhancement (H) 379](#_Toc522289386)

[SI-6 Security Functionality Verification (M) (H) 379](#_Toc522289387)

[SI-7 Software & Information Integrity (M) (H) 381](#_Toc522289388)

[SI-7 (1) Control Enhancement (M) (H) 381](#_Toc522289389)

[SI-7 (2) Control Enhancement (H) 382](#_Toc522289390)

[SI-7 (5) Control Enhancement (H) 383](#_Toc522289391)

[SI-7 (7) Control Enhancement (M) (H) 384](#_Toc522289392)

[SI-7 (14) Control Enhancement (H) 385](#_Toc522289393)

[SI-8 Spam Protection (M) (H) 385](#_Toc522289394)

[SI-8 (1) Control Enhancement (M) (H) 386](#_Toc522289395)

[SI-8 (2) Control Enhancement (M) (H) 387](#_Toc522289396)

[SI-10 Information Input Validation (M) (H) 388](#_Toc522289397)

[SI-11 Error Handling (M) (H) 388](#_Toc522289398)

[SI-12 Information Output Handling and Retention (L) (M) (H) 389](#_Toc522289399)

[SI-16 Memory Protection (M) (H) 390](#_Toc522289400)

[14. Acronyms 392](#_Toc522289401)

[15. Attachments 393](#_Toc522289402)

[Attachment 1 Information Security Policies and Procedures 395](#_Toc522289403)

[Attachment 2 User Guide 396](#_Toc522289404)

[Attachment 3 Digital Identity Worksheet 397](#_Toc522289405)

[Introduction and Purpose 397](#_Toc522289406)

[Information System Name/Title 397](#_Toc522289407)

[Digital Identity Level Definitions 397](#_Toc522289408)

[Review Maximum Potential Impact Levels 398](#_Toc522289409)

[Digital Identity Level Selection 399](#_Toc522289410)

[Attachment 4 PTA/PIA 400](#_Toc522289411)

[Privacy Overview and Point of Contact (POC) 400](#_Toc522289412)

[Applicable Laws and Regulations 400](#_Toc522289413)

[Applicable Standards and Guidance 401](#_Toc522289414)

[Personally Identifiable Information (PII) 401](#_Toc522289415)

[Privacy Threshold Analysis 402](#_Toc522289416)

[Qualifying Questions 402](#_Toc522289417)

[Designation 402](#_Toc522289418)

[Attachment 5 Rules of Behavior 403](#_Toc522289419)

[Attachment 6 Information System Contingency Plan 404](#_Toc522289420)

[Attachment 7 Configuration Management Plan 405](#_Toc522289421)

[Attachment 8 Incident Response Plan 406](#_Toc522289422)

[Attachment 9 CIS Workbook 407](#_Toc522289423)

[Attachment 10 FIPS 199 408](#_Toc522289424)

[Introduction and Purpose 408](#_Toc522289425)

[Scope 408](#_Toc522289426)

[System Description 408](#_Toc522289427)

[Methodology 409](#_Toc522289428)

[Attachment 11 Separation of Duties Matrix 411](#_Toc522289429)

[Attachment 12 FedRAMP Laws and Regulations 412](#_Toc522289430)

[Attachment 13 FedRAMP Inventory Workbook 413](#_Toc522289431)

List of Figures

[Figure 9‑1. Authorization Boundary Diagram 10](#_Toc522289432)

[Figure 9‑2. Network Diagram 12](#_Toc522289433)

[Figure 10‑1. Data Flow Diagram 13](#_Toc522289434)

List of Tables

[Table 1‑1. Information System Name and Title 1](#_Toc522289435)

[Table 2‑1. Security Categorization 1](#_Toc522289436)

[Table 2‑2. Sensitivity Categorization of Information Types 3](#_Toc522289437)

[Table 2‑3. Security Impact Level 3](#_Toc522289438)

[Table 2‑4. Baseline Security Configuration 3](#_Toc522289439)

[Table 3‑1. Information System Owner 4](#_Toc522289440)

[Table 5‑1. Information System Management Point of Contact 5](#_Toc522289441)

[Table 5‑2. Information System Technical Point of Contact 5](#_Toc522289442)

[Table 6‑1. CSP Name Internal ISSO (or Equivalent) Point of Contact 6](#_Toc522289443)

[Table 6‑2. AO Point of Contact 6](#_Toc522289444)

[Table 7‑1. System Status 6](#_Toc522289445)

[Table 8‑1. Service Layers Represented in this SSP 7](#_Toc522289446)

[Table 8‑2. Cloud Deployment Model Represented in this SSP 8](#_Toc522289447)

[Table 8‑3. Leveraged Authorizations 8](#_Toc522289448)

[Table 9‑1. Personnel Roles and Privileges 10](#_Toc522289449)

[Table 10‑1. Ports, Protocols and Services 14](#_Toc522289450)

[Table 11‑1. System Interconnections 15](#_Toc522289451)

[Table 12‑1. Information System Name Laws and Regulations 17](#_Toc522289452)

[Table 12‑2. Information System Name Standards and Guidance 17](#_Toc522289453)

[Table 13‑1. Summary of Required Security Controls 18](#_Toc522289454)

[Table 13‑2. Control Origination and Definitions 24](#_Toc522289455)

[Table 13‑3. CA-3 Authorized Connections 108](#_Toc522289456)

[Table 15‑1. Names of Provided Attachments 394](#_Toc522289457)

[Table 15‑2. Information System Name and Title 397](#_Toc522289458)

[Table 15‑3. Mapping FedRAMP Levels to NIST SP 800-63-3 Levels 398](#_Toc522289459)

[Table 15‑4. Potential Impacts for Assurance Levels 399](#_Toc522289460)

[Table 15‑5. Digital Identity Level 399](#_Toc522289461)

[Table 15‑6. Information System Name; Privacy POC 400](#_Toc522289462)

[Table 15‑7. <Information System Name> Laws and Regulations 401](#_Toc522289463)

[Table 15‑8. <Information System Name> Standards and Guidance 401](#_Toc522289464)

[Table 15‑9. CSP Applicable Information Types with Security Impact Levels Using NIST SP 800-60 V2 R1 410](#_Toc522289465)

[Table 15‑10. FedRAMP Templates that Reference FedRAMP Laws and Regulations Standards and Guidance 412](#_Toc522289466)

System Security Plan Approvals

Cloud Service Provider Signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
| Name | James Spiridopoulos | | Date | <Select Date> |
| Title | System Security Plan Approval | | | |
| Cloud Service Provider | | GDIT | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Peter Harroun | | Date | <Select Date> |
| Title | System Security Plan Approval | | | |
| Cloud Service Provider | | GDIT | | |
|  | | | | |
|  | | | | |
|  | | | | |
| Name | Peter Harroun | | Date | <Select Date> |
| Title | Information System Owner | | | |
| Cloud Service Provider | | GDIT | | |
|  | |  | | |

# 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: | high |

## 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 | high |

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.

# 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 | James Spiridopoulos |
| Title | Information System Owner |
| Company / Organization | General Dynamics Information Technology |
| Address | 11400 Westmoor Circle Suite 1500 Westminster CO 80021 US |
| Phone Number | 703-582-3749 |
| Email Address | James.Spiridopoulos@GDIT.com |

# Authorizing Officials

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

Table 6‑2. AO Point of Contact

| **AO Point of Contact** | |
| --- | --- |
| Name | James Spiridopoulos |
| Title | Authorizing Official |
| Organization | General Dynamics Information Technology |
| Address | 11400 Westmoor Circle Suite 1500 Westminster CO 80021 US |
| Phone Number | 703-582-3749 |
| Email Address | James.Spiridopoulos@GDIT.com |

# 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. cAdd 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 types. (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 | P | 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

## 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 GDIT 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 GDIT 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 GDIT. | 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 GDIT 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 GDIT 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 (H)

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 annually]; and
   2. Access control procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| **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 | These policies are stored in the GDIT Cloud's secure SharePoint site. |
| Part b1 | 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 (H)

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: monthly for privileged accessed, every six (6) months for non-privileged access]; 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 | Customers are responsible for identifying and selecting the types of information system accounts to support organizational missions/business functions in the Customer environment. |
| Part b | The process is associated with the staffing activity and associated role assignment where the System Manager creates a ticket in Cherwell to create a task for the AD administrator to assign the account managers the ability to manage the accounts in their respective areas of responsibility. |
| Part c | During the on-boarding process, Account Managers determine the role(s) for each team member to link their individual account to a proper AD permission group and then to create a ticket in Cherwell to have an individual assigned a role(s) that contains the access privileges associated in Attachment 10: Roles and Privileges Matrix. |
| Part d | Once the System Manager and ISSO have approved the account, the system administrator establishes and activates the account and distributes the credentials. |
| Part e | The account request ticket is then forwarded to the AD system administrator, who creates the user account in the GDIT Cloud AD system. |
| Part f | The Customer system administrator is responsible for creating, enabling, modifying, disabling, and removing users’ accounts within the Customer environment. |
| Part g | 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 | 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 | GDIT Cloud accounts created. |
| Part j | 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 | Customers are responsible for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. |

#### AC-2 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the management of information system accounts.

| **AC-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 | |

|  |
| --- |
| AC-2 (1) What is the solution and how is it implemented? |
| Click or tap here to enter text. |

#### AC-2 (2) Control Enhancement (H)

The information system automatically [FedRAMP Selection: disables] temporary and emergency accounts after [FedRAMP Assignment: 24 hours from last use].

| **AC-2 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter AC-2(2)1: removes; disables | |
| Parameter AC-2(2)2: within 24 hours for all account types | |
| 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 (2) What is the solution and how is it implemented?** |
| GDIT Cloud does not employ temporary local accounts. |

#### AC-2 (3) Control Enhancement (H)

The information system automatically disables inactive accounts after [FedRAMP Assignment: thirty-five (35) days for user accounts].

AC-2 (3) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the JAB/AO. Where user management is a function of the service, reports of activity of consumer users shall be made available.

| **AC-2 (3)** | **Control Enhancement Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter AC-2(3): Assignment: 90 days for user 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 | |

|  |
| --- |
| **AC-2 (3) What is the solution and how is it implemented** |
| ‘Inactivity’ in this report is triggered by the Active Directory days since last password change. This is due to users that use only the Cherwell web service do not trigger an update to the ‘Last Login’ variable. |

#### AC-2 (4) Control Enhancement (H)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [FedRAMP Assignment: organization and/or service provider system owner].

| **AC-2 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter AC-2(4): on-duty security analyst | |
| 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 (4) What is the solution and how is it implemented?** |
| System Administrators configure AD to automatically audit account creation, modification, enabling, disabling, and removal actions by recording the event and sending to the SIEM, which also generates a ticket in Cherwell that routes it to the Security Operations Center (SOC) for investigation. The on-duty analyst then works the ticket to closure and determines if this were an approved, authorized change or an incident. |

#### AC-2 (5) Control Enhancement (H)

The organization requires that users log out when [FedRAMP Assignment: inactivity is anticipated to exceed fifteen (15) minutes].

**AC-2 (5) Additional FedRAMP Requirements and Guidance:**

Guidance: Should use a shorter timeframe than AC-12

| **AC-2 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-2(5): 15 minutes | |
| 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 (5) What is the solution and how is it implemented?** |
| See also AC-11 for the technical controls to enforce a logout/disconnect after 15 minutes of inactivity. |

#### AC-2 (7) Control Enhancement (H)

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [FedRAMP Assignment: disables//revokes access within an organization-specified timeframe] when privileged role assignments are no longer appropriate.

|  |  |
| --- | --- |
| **AC-2 (7)** | **Control Summary Information** |
| Responsible Role: Security Analysts | |
| Parameter AC-2(7)(c): Disables | |
| 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 (7) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | The Customer is responsible for defining the roles and responsibilities of users in the customer environment, based on the customer-defined access scheme that organizes information system and network access into roles and tracks and monitors privileged role assignments. |
| Part b | The Customer is responsible for defining the roles and responsibilities of Customer users of the GDIT Cloud based on customer-defined access scheme that organizes information system and network access into roles and tracks and monitors privileged (provisioning) role assignments. |
| Part c | When the System Manager determines that a privileged role assignment is no longer appropriate, he or she opens a ticket in Cherwell to disable the account and remove the role from the user account in AD. |

#### AC-2 (9) Control Enhancement (H)

The organization only permits the use of shared/group accounts that meet [FedRAMP Assignment: organization-defined need with justification statement that explains why such accounts are necessary].

AC-2 (9) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

| **AC-2 (9)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter AC-2(9): GDIT Cloud-defined conditions for establishing shared/group accounts: None | |
| 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 (9) What is the solution and how is it implemented?** |
| Break Glass (Administrator) account has FULL access to Domain Controllers, all member servers, and devices that are bound to the Active Directory. This emergency account password is kept in the Password Manager Pro application to support disaster/recovery scenarios. |

#### AC-2 (10) Control Enhancement (M) (H)

The information system terminates shared/group account credentials when members leave the group.

AC-2 (10) Additional FedRAMP Requirements and Guidance: Required if shared/group accounts are deployed.

| **AC-2 (10)** | **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 | |

|  |
| --- |
| **AC-2 (10) What is the solution and how is it implemented?** |
| This control is N/A. According to GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.1, no Group or Shared individual accounts are allowed within the GDIT Cloud environment, i.e., no instance of a single group account with a shared logon and password for an individual. |

#### AC-2 (11) Control Enhancement (H)

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined information system accounts].

| **AC-2 (11)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-2 (11)-1: Click or tap here to enter text. | |
| Parameter AC-2 (11)-2: Click or tap here to enter text. | |
| 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 (11) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-2 (12) Control Enhancement (H)

The organization:

1. Monitors information system accounts for [Assignment: organization-defined atypical use]; and
2. Reports atypical usage of information system accounts to [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization].

AC-2 (12) (a) and AC-2 (12) (b) Additional FedRAMP Requirements and Guidance: Required for privileged accounts.

| **AC-2 (12)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter AC-2(12)(a): unauthorized changes, privilege escalation attempts, attempting to log into unauthorized resources | |
| Parameter AC-2(12)(b): Security Analyst in the SOC | |
| 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 (12) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Additional information on system monitoring can be found under SI-4. |
| Part b | The SIEM generates alerts that are sent to Security Analysts when atypical usage is detected. The alert is sent to both the AlienVault console and Cherwell as an Event. Cherwell automatically generates a ticket. Security Analysts investigate the alert and either determine it is authorized by reviewing Cherwell Service Requests or the Event becomes a Security Incident and follows the controls described in IR-4 Incident Handling within this document. |

#### AC-2 (13) Control Enhancement (H)

The organization disables accounts of users posing a significant risk within [FedRAMP Assignment: one (1) hour] of discovery of the risk.

| **AC-2 (13)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-2 (13): Click or tap here to enter text. | |
| 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 (13) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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 Authorization | |

| **AC-3 What is the solution and how is it implemented?** |
| --- |
| 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-4 Information Flow Enforcement (M) (H)

The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies].

| **AC-4** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter AC-4: Program-defined information flow control policies | |
| 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-4 What is the solution and how is it implemented?** |
| --- |
| The customer is responsible for enforcing approved authorizations for controlling the flow of information within its Customer environment and between interconnected systems in accordance with applicable policy. |

#### AC-4 (8) Control Enhancement (H)

The information system enforces information flow control using [Assignment: organization-defined security policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows].

| **AC-4 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-4 (8)-1: Click or tap here to enter text. | |
| Parameter AC-4 (8)-2: Click or tap here to enter text. | |
| 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-4 (8) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-4 (21) Control Enhancement (M) (H)

The information system separates information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].

| **AC-4 (21)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter AC-4 (21)-1: distinct virtual local area networks (VLANS) | |
| Parameter AC-4 (21)-2: separations by types of information:; Out of Band Management; Toll Free Numbers; Session Border Controller; Program Tenant; Program Enclaves | |
| 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-4 (21) What is the solution and how is it implemented?** |
| --- |
| Any change to the VLAN configuration is controlled by the GDIT Change Management processes, and only GDIT Cloud network engineers are allowed to make the change as directed by the CAB. |

### AC-5 Separation of Duties (M) (H)

The organization:

1. Separates [Assignment: organization-defined duties of individuals];
2. Documents separation of duties of individuals; and
3. Defines information system access authorizations to support separation of duties.

AC-5 Additional FedRAMP Requirements and Guidance:

Guidance: CSPs have the option to provide a separation of duties matrix as an attachment to the SSP. Directions for attaching the Separation of Duties Matrix document may be found in Attachment 11, Separation of Duties Matrix.

| **AC-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-5(a): GDIT Cloud-defined duties of individuals | |
| 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-5 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | The System Manager is responsible for separating duties to specific roles in the GDIT Cloud environment. Specifically, each role, assigned to a privileged user in AD, grants access authorization to perform specific duties in the Cloud environment, as defined in the GDIT Cloud Roles and Privileges Matrix in Attachment 10. |
| Part b | The System Manager has documented the separation of duties as part of the assigned roles and responsibilities in the GDIT Cloud Roles and Privileges Matrix in Attachment 10. |
| Part c | Customers are responsible for separating, documenting, and defining separation of duties within the Customer environment. |

### AC-6 Least Privilege (M) (H)

The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

| **AC-6** | **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-6 What is the solution and how is it implemented?** |
| --- |
| Once the System Manager defines roles according to the principle of least privilege, System Administrators apply the policy in Active Directory defining group permissions that restrict users to specific roles and access permissions. |

#### AC-6 (1) Control Enhancement (H)

The organization explicitly authorizes access to [FedRAMP Assignment: all functions not publicly accessible and all security-relevant information not publicly available].

| **AC-6 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter AC-6 (1): organization-defined security functions and security-relevant information:; Create/Modify/Delete Admin User(s); Create/Modify/Delete Non-Admin User(s); Modify Device Audit configuration; Modify System Security Parameters; Add/Change/Delete Firewall ACL’s; Configuration of Intrusion Detection and Prevention (IDP) alerts and Exclusions; Add/Change/Delete Network Switch configuration; Establish a remote connection to the device (SSH/VPN) | |
| 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-6 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-6 (2) Control Enhancement (M) (H)

The organization requires that users of information system accounts, or roles, with access to [FedRAMP Assignment: all security functions], use non-privileged accounts or roles, when accessing non-security functions.

AC-6 (2) Additional FedRAMP Requirements and Guidance: Examples of security functions include but are not limited to: establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters, system programming, system and security administration, other privileged functions.

| **AC-6 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-6 (2)All security functions | |
| 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-6 (2) What is the solution and how is it implemented?** |
| --- |
| However, GDIT Cloud personnel withprivilegedaccess do not conduct other non-privileged activities while administeringthe system andtherefore are not granted non-privileged accounts. |

#### AC-6 (3) Control Enhancement (H)

The organization authorizes network access to [FedRAMP Assignment: all privileged commands] only for [Assignment: organization-defined compelling operational needs] and documents the rationale for such access in the security plan for the information system.

| **AC-6 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-6 (3)-1: Click or tap here to enter text. | |
| Parameter AC-6 (3)-2: Click or tap here to enter text. | |
| 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-6 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC 6 (5) Control Enhancement (M) (H)

The organization restricts privileged accounts on the information system to [Assignment: organization-defined personnel or roles].

| **AC-6 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Account Manager | |
| Parameter AC-6 (5): GDIT Cloud 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 | |

| **AC-6 (5) What is the solution and how is it implemented?** |
| --- |
| System Administrators configure MS Active Directory group permissions to restrict users to specific roles and the permissions. Additionally, roles and accesses for personnel are reviewed prior to approval through the on-boarding process. |

#### AC-6 (7) Control Enhancement (H)

The organization:

1. Reviews [FedRAMP Assignment: at a minimum, annually] the privileges assigned to [FedRAMP Assignment: all users with privileges] to validate the need for such privileges; and
2. Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

| **AC-6 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-6 (7)(a)-1: Click or tap here to enter text. | |
| Parameter AC-6 (7)(b)-2: Click or tap here to enter text. | |
| 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-6 (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. |

#### AC-6 (8) Control Enhancement (H)

The information system prevents [FedRAMP Assignment: any software except software explicitly documented] from executing at higher privilege levels than users executing the software.

| **AC-6 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-6 (8): Click or tap here to enter text. | |
| 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-6 (8) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-6 (9) Control Enhancement (M) (H)

The information system audits the execution of privileged functions.

| **AC-6 (9)** | **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 | |

| **AC-6 (9) What is the solution and how is it implemented?** |
| --- |
| Security Engineers configured the system as part of AU-2d. and AU-12 to ensure that privileged functions are audited. Tripwire provides verification that the systems are configured to audit privileged functions. |

#### AC-6 (10) Control Enhancement (M) (H)

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

| **AC-6 (10)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Account Managers | |
| 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-6 (10) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### AC-7 Unsuccessful Login Attempts (H)

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: minimum of three (3) hours or until unlocked by an administrator]; 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 | 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 | 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-7 (2) Control Enhancement (H)

The information system purges/wipes information from [FedRAMP Assignment: mobile devices as defined by organization policy] based on [Assignment: organization-defined purging/wiping requirements/techniques] after [FedRAMP Assignment: three (3)] consecutive, unsuccessful device logon attempts.

| **AC-7 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-7(2)-1: Click or tap here to enter text. | |
| Parameter AC-7(2)-2: Click or tap here to enter text. | |
| Parameter AC-7(2)-3: Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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 | \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 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 | 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: 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 Authorization | |

| **AC-8 What is the solution and how is it implemented?** | |
| --- | --- |
| Req. 1 | The customer is responsible for ensuring that a system usenotification warning banner is verified on all of their systems within their environments. |
| Req. 2 | 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-10 Concurrent Session Control (M) (H)

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [FedRAMP Assignment: three (3) sessions for privileged access and two (2) sessions for non-privileged access].

| **AC-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter AC-10-1: three (3) sessions for privileged access and two (2) sessions for non-privileged access | |
| Parameter AC-10-2: Click or tap here to enter text. | |
| 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-10 What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### AC-11 Session Lock (M) (H)

The information system:

1. Prevents further access to the system by initiating a session lock after [FedRAMP Assignment: fifteen (15) minutes] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

| **AC-11** | **Control Summary Information** |
| --- | --- |
| Responsible Role: GDIT Cloud System Administrator | |
| Parameter AC-11(a): fifteen minutes | |
| 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-11 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Mitigation: The room where the workstations reside is a controlled access point. |
| Part b | The GDIT Cloud systemprevents further accesstothe system by initiatingasessionlockthat remainsin effectuntilthe user reestablishes accessusing appropriate identification and authenticationprocedures. |

#### AC-11 (1) Control Enhancement (M) (H)

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

| **AC-11 (1)** | **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 | |

| **AC-11 (1) What is the solution and how is it implemented?** |
| --- |
| System Administrators configure the GDIT Cloud system to redirect to a session locked screen after the session lock has been activated. This redirection is a configuration setting in the group policy and the selection of the public viewable screen is also a setting. On the next user activity the user is redirect to the login page. |

### AC-12 Session Termination (M) (H)

The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].

| **AC-12** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter AC-12: 15 minutes of 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 | |

| **AC-12 What is the solution and how is it implemented?** |
| --- |
| All GDIT Cloud workstations are configured through group policy GPO to perform the lockout. |

#### AC-12 (1) Control Enhancement (H)

The information system:

1. Provides a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources]; and
2. Displays an explicit logout message to users indicating the reliable termination of authenticated communications sessions.

AC-8 Additional FedRAMP Requirements and Guidance:

Guidance: Testing for logout functionality (OTG-SESS-006) https://www.owasp.org/index.php/Testing\_for\_logout\_functionality\_%28OTG-SESS-006%29

| **AC-12 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AC-12 (1)(a): Click or tap here to enter text. | |
| 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-12 (1) What is the solution and how is it implemented?** |
| --- |
| 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 Authorization | |

| **AC-17 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Implementation Guidance: HTTPS and FIPS 140-2 encryption and 2- factor authentication |
| Part b | 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-17 (1) Control Enhancement (M) (H)

The information system monitors and controls remote access methods.

| **AC-17 (1)** | **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 | |

| **AC-17 (1) What is the solution and how is it implemented?** |
| --- |
| There are automated mechanisms in AlienVault to facilitatethemonitoring and control (using firewalls in conjunction with RSA and AD) of remote accessmethods. |

#### AC-17 (2) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

| **AC-17 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network 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 | |

| **AC-17 (2) What is the solution and how is it implemented?** |
| --- |
| The Web Portal ITSM tool connecting over HTTP is automatically redirected to HTTPS to protect the confidentiality and integrity of remote access sessions |

#### AC-17 (3) Control Enhancement (M) (H)

The information system routes all remote accesses through [Assignment: organization-defined number] managed network access control points.

| **AC-17 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter AC-17(3): single | |
| 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-17 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-17 (4) Control Enhancement (M) (H)

The organization:

1. Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [Assignment: organization-defined needs]; and
2. Documents the rationale for such access in the security plan for the information system.

| **AC-17 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-17 (4)(a): organization-defined needs:; Problem or incident; Required after-hours work | |
| 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-17 (4) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Required after-hours work that is authorized by the Operations Manager for remote access (non-emergency) |
| Part b | The ISSO documents the rationale for such access in this security plan. Authorization to systems is dependent on the user’s role as defined by user attributes stored in MS Active Directory. These attributes indicate the status of employee / customer / contractor. Depending on the system access privileges in AD, the users are permitted access to different network, software, and hardware component. |

#### AC-17 (9) Control Enhancement (M) (H)

The organization provides the capability to expeditiously disconnect or disable remote access to the information system within [FedRAMP Assignment: fifteen (15) minutes].

| **AC-17 (9)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Analyst | |
| Parameter AC-17 (9): no greater than fifteen minutes | |
| 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-17 (9) What is the solution and how is it implemented?** |
| --- |
| Reasons for needing an immediate disconnect are not covered in this section. This capability provides additional response capabilities for SI-4(a)[1] and SI-4(a)[2]. |

### 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-18 (1) Control Enhancement (M) (H)

The information system protects wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.

| **AC-18 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter AC-18 (1): users; devices | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| The GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.1 prohibits wireless access points. The GDIT Cloud protects wireless access to the system through not allowing wireless access points. |

#### AC-18 (3) Control Enhancement (H)

The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.

| **AC-18 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-18 (4) Control Enhancement (H)

The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities.

| **AC-18 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AC-18 (5) Control Enhancement (H)

The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

| **AC-18 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (5) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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 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 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-19 (5) Control Enhancement (M) (H)

The organization employs [Selection: full-device encryption; container encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].

| **AC-19 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter AC-19 (5)-1: full-device encryption; container encryption | |
| Parameter AC-19 (5)-2: None | |
| 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 (5) What is the solution and how is it implemented?** |
| --- |
| Once a laptop is joined to the domain, it inherits hardening based on its location within the environment. |

### 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 | Customer agencies are responsible for establishing and managing terms and conditions for the use of external systems within their environment. |
| Part b | 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-20 (1) Control Enhancement (M) (H)

The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

1. Verifies the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or
2. Retains approved information system connection or processing agreements with the organizational entity hosting the external information system.

| **AC-20 (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)  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 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Customer agencies are responsible for authorizing individuals to use an external information system to access their information system and manage the information system connection. |
| Part b | Customer agencies are responsible for processing agreements with the organizational entity hosting the external information system. |

#### AC-20 (2) Control Enhancement (M) (H)

The organization [Selection: restricts; prohibits] the use of organization-controlled portable storage devices by authorized individuals on external information systems.

| **AC-20 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-20 (2): Prohibits | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| KA 10668 - Approved Removable Media Check-out SOP and Inventory, KA 10693 - How To: Request USB Storage . Though these hard drives are FIPS 140-2 Level 3 validated, the operations team does not process PII, PCI, PHA, or Classified Information of any kind inside the GDIT Cloud infrastructure. The SOC works with customer POCs to ensure exposure of these types of data do not occur within the Tech Services FedRAMP boundary. This includes all SOC and NOC workstations. Before initiating and upon completion of each Service Request, SOC analyst sanitizes the drives to a zero state. Through the life of the request, Knowledge Article 10666 – “GDIT Cloud Chain of Custody Form ” applies. |

### AC-21 Information Sharing (M) (H)

The organization:

1. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
2. Employs [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing/collaboration decisions.

| **AC-21** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AC-21(a): Need to know basis where user discretion is required | |
| Parameter AC-21(b): manual processes | |
| 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-21 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | The System Manager has determined that all GDIT Cloud documentation will be maintained on the secure GDIT Cloud SharePoint site that is accessible only to authorized personnel. |
| Part b | In both cases, the request is forwarded to the ISSO, who accepts or rejects the request, based on whether the requestor is a GD employee or contractor and has demonstrated a need-to-know. If accepted, the GDIT Cloud system administrator grants access to the requestor to the Cloud information on SharePoint. |

### 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 (H)

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 annually*]; and
   2. Security awareness and training procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **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 | All procedures are stored in an access controlled GDIT Cloud SharePoint site where version control is maintained. |
| Part b | 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 | Note: GDIT may modify the contents to emphasize emerging threats. |
| Part b | 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 | 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-2 (2) Control Enhancement (M) (H)

The organization includes security awareness training on recognizing and reporting potential indicators of insider threat.

| **AT-2 (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 | |

| **AT-2 (2) What is the solution and how is it implemented?** |
| --- |
| The training also includes how employees are to communicate to management concerns regarding potential indicators of insider threats. |

### 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 | 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 | Click or tap here to enter text. |
| Part c | 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-3 (3) Control Enhancement (H)

The organization includes practical exercises in security training that reinforce training objectives.

| **AT-3 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AT-3 (4) Control Enhancement (H)

The organization provides training to its personnel on [FedRAMP Assignment: malicious code indicators as defined by organization incident policy/capability] to recognize suspicious communications and anomalous behavior in organizational information systems.

| **AT-3 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AT-3 (4): Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### AT-4 Security Training Records (H)

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 five (5) years or 5 years after completion of a specific training program].

| **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 | 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 (H)

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 least annually*]; and
   2. Audit and accountability procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

| **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 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 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 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 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 | Permission changes can be an indicator of compromise or attempted compromise when the change were made without authorization. |
| Part d | These events are a subset of the auditable events listed in AU-2a. and are configured as part of control AU-12. |

#### AU-2 (3) Control Enhancement (M) (H)

The organization reviews and updates the audited events [FedRAMP Assignment: annually or whenever there is a change in the threat environment].

AU-2 (3) Additional FedRAMP Requirements and Guidance:

Guidance: Annually or whenever changes in the threat environment are communicated to the service provider by the JAB/AO.

| **AU-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Analysts | |
| Parameter AU-2 (3): annually or whenever there is a change in the threat environment and whenever changes in the threat environment are communicated to the ISSO and/or Cloud System Administrators 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 | |

| **AU-2 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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?** |
| --- |
| Click or tap here to enter text. |

#### AU-3 (1) Control Enhancement (H)

The information system generates audit records containing the following additional information: [FedRAMP Assignment: organization-defined additional, more detailed information].

AU-3 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines audit record types [FedRAMP Assignment: session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon; individual identities of group account users; full-text of privileged commands]. The audit record types are approved and accepted by the JAB/AO.

Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry.

| **AU-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter AU-3 (1): session, connection, transaction, or activity duration; for client-server transactions, the number of bytes received and bytes sent; additional informational messages to diagnose or identify the event; characteristics that describe or identify the object or resource being acted upon. The service provider defines audit record types. The audit record types are approved and accepted by the JAB. Guidance: For client-server transactions, the number of bytes sent and received gives bidirectional transfer information that can be helpful during an investigation or inquiry. | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| cisco-asa.log:Dec 12 16:56:46 10.68.255.4 %ASA-5-113005: AAA user authentication Rejected : reason = Unspecified : server = 10.68.67.119 : user = techservices\shadyinternetguy |

#### AU-3 (2) Control Enhancement (H)

The information system provides centralized management and configuration of the content to be captured in audit records generated by [FedRAMP Assignment: all network, data storage, and computing devices].

| **AU-3 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-3 (2): Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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?** |
| --- |
| On a semi-annual basis, the Security Engineer reviews the total usage and adjusts the storage capacity to reduce the likelihood of exceeding capacity. |

### 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 | 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 | 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-5 (1) Control Enhancement (H)

The information system provides a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit record storage capacity.

| **AU-5 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-5 (1)-1: Click or tap here to enter text. | |
| Parameter AU-5 (1)-2: Click or tap here to enter text. | |
| Parameter AU-5 (1)-3: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-5 (2) Control Enhancement (H)

The information system provides an alert in [FedRAMP Assignment: organization-defined real-time] to [FedRAMP Assignment: service provider personnel with authority to address failed audit events] when the following audit failure events occur: [FedRAMP Assignment: audit failure events requiring real-time alerts, as defined by organization audit policy].

| **AU-5 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-5 (1)-1: Click or tap here to enter text. | |
| Parameter AU-5 (1)-2Click or tap here to enter text. | |
| Parameter AU-5 (1)-3Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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 | 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-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

| **AU-6 (1)** | **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 | |

| **AU-6 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-6 (3) Control Enhancement (M) (H)

The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.

| **AU-6 (3)** | **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 | |

| **AU-6 (3) What is the solution and how is it implemented?** |
| --- |
| The SIEM tool receives logging information from every repository via installed agents and syslog on the remote devices. The data is consolidated to one central repository by the SIEM tool. The SIEM tool provides over 15,000 signatures to correlate the log events. The Security Engineers code additional correlation rules as indicated and approved by weekly meetings, Lessons Learned from security incidents, and changes in the threat environment communicated by the JAB. |

#### AU-6 (4) Control Enhancement (H)

The information system provides the capability to centrally review and analyze audit records from multiple components within the system.

| **AU-6 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-6 (5) Control Enhancement (H)

The organization integrates analysis of audit records with analysis of [FedRAMP Selection (one or more): vulnerability scanning information; performance data; information system monitoring information; penetration test data; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.

| **AU-6 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-6 (5): Click or tap here to enter text. | |
| 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 (5) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-6 (6) Control Enhancement (H)

The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

AU-6 Additional FedRAMP Requirements and Guidance:

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

| **AU-6 (6)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (6) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-6 (7) Control Enhancement (H)

The organization specifies the permitted actions for each [FedRAMP Selection (one or more): information system process; role; user] associated with the review, analysis, and reporting of audit information.

| **AU-6 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-6 (7): Click or tap here to enter text. | |
| 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 (7) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-6 (10) Control Enhancement (H)

The organization adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

| **AU-6 (10)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (10) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### AU-7 Audit Reduction and Report Generation (M) (H)

The information system provides an audit reduction and report generation capability that:

1. Supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incidents; and
2. Does not alter the original content or time ordering of audit records.

| **AU-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security 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-7 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | To allowthe user to select event criteria(typeof log, host name, IP address, username, or port number) in order to further investigate specific time periods, events or suspicious activity. |
| Part b | Security Engineers have configured the GDIT Cloud MMS SIEM to alert on systemconfiguration changes and user account creations,deletions, and modifications. In this way, the GDIT Cloud guards against alteringoriginal records that support after-the-fact investigations. This includes monitoring for any alteration of the original content or time ordering of audit records. |

#### AU-7 (1) Control Enhancement (M) (H)

The information system provides the capability to process audit records for events of interest based on [Assignment: organization-defined audit fields within audit records].

| **AU-7 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter AU-7 (1): correlation rules (event criteria) | |
| 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-7 (1) What is the solution and how is it implemented?** |
| --- |
| Security Engineers can add and modify the existing correlation rules in response to notifications based on risk. The GDIT Cloud Security Staff holds a weekly Security Operations review meeting where incidents and trends are reviewed and evaluated for process and support improvements. |

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

The information system:

1. Compares the internal information system clocks with [FedRAMP Assignment: authoritative time source: [[*http://tf.nist.gov/tf-cgi/servers.cgi*](http://tf.nist.gov/tf-cgi/servers.cgi)] [at least hourly]]; and
2. Synchronizes the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].

AU-8 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider selects primary and secondary time servers used by the NIST Internet time service. The secondary server is selected from a different geographic region than the primary server.

Requirement: The service provider synchronizes the system clocks of network computers that run operating systems other than Windows to the Windows Server Domain Controller emulator or to the same time source for that server.

Guidance: The service provider selects primary and secondary time servers used by the NIST Internet time service, or by a Stratum-1 time server. The secondary server is selected from a different geographic region than the primary server.

If using Windows Active Directory, all servers should synchronize time with the time source for the Windows Domain Controller. If using some other directory services (e.g., LDAP), all servers should synchronize time with the time source for the directory server. Synchronization of system clocks improves the accuracy of log analysis.

| **AU-8 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter AU-8(1)(a)-1: at least hourly | |
| Parameter AU-8(1)(a)-2: http://tf.nist.gov/tf-cgi/servers.cgi | |
| Parameter AU-8(1)(b): Sync is hourly | |
| 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 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | System Administrators configure all devices in the GDIT Cloud to point to the redundant NTP Stratum 1 time servers which they leverage to set their system time. The GDIT Cloud components validate their time with the NTP servers at least hourly. The Hypervisors pass on this NTP-managed system time to the VM’s they host. |
| Part b | System Administrators configure all devices to use NTP updated local clocks to time stamp audit records and maintain system time. The GDIT Cloud leverages two internal Stratum 1 Appliances that utilize redundant power sources and redundant network segments to provide synchronization. |

### 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?** |
| --- |
| 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-9 (2) Control Enhancement (M) (H)

The information system backs up audit records [FedRAMP Assignment: at least weekly] onto a physically different system or system component than the system or component being audited.

| **AU-9 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter AU-9(2): Weekly | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| Performs backups nightly between Westminster and Manassas |

#### AU-9 (3) Control Enhancement (H)

The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

| **AU-9 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-9 (4) Control Enhancement (M) (H)

The organization authorizes access to management of audit functionality to only [Assignment: organization-defined subset of privileged users].

| **AU-9 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter AU-9(4): SOC 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 | |

| **AU-9 (4) What is the solution and how is it implemented?** |
| --- |
| The Security Analyst is able to monitor such changes in the system through the use of AlienVault. This allows detection of misuse of the privileged authority. |

### AU-10 Non-repudiation (H)

The information system protects against an individual (or process acting on behalf of an individual) falsely denying having performed [FedRAMP Assignment: minimum actions including the addition, modification, deletion, approval, sending, or receiving of data].

| **AU-10** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-10: Click or tap here to enter text. | |
| 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-10 What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### AU-11 Audit Record Retention (H)

The organization retains audit records for [FedRAMP Assignment: at least one (1) year] 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?** |
| --- |
| 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 | 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. |

#### AU-12 (1) Control Enhancement (H)

The information system compiles audit records from [FedRAMP Assignment: all network, data storage, and computing devices] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail].

| **AU-12 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-12 (1)-1: Click or tap here to enter text. | |
| Parameter AU-12 (1)-2: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### AU-12 (3) Control Enhancement (H)

The information system provides the capability for [FedRAMP Assignment: service provider-defined individuals or roles with audit configuration responsibilities] to change the auditing to be performed on [FedRAMP Assignment: all network, data storage, and computing devices] based on [Assignment: organization-defined threat situations] within [Assignment: organization-defined time thresholds].

| **AU-12 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter AU-12 (3)-1: Click or tap here to enter text. | |
| Parameter AU-12 (3)-2: Click or tap here to enter text. | |
| Parameter AU-12 (3)-3: Click or tap here to enter text. | |
| Parameter AU-12 (3)-4: Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

## Security Assessment and Authorization (CA)

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

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 annually*]; and
   2. Security assessment and authorization procedures [*FedRAMP Assignment: at least at least annually or whenever a significant change occurs*].

| **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 policy and procedures documents are stored in the secure GDIT Cloud SharePoint site, which maintains change history and version control. |
| Part b | 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 | Once completed, the 3PAO submits the SAP to the FedRAMP PMO for approval in the timeline dictated by the PMO for reaccreditation. |
| Part b | 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 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 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?** |
| --- |
| Provides the results of the security control assessment, in writing, to the FedRAMP JAB. |

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

The organization includes as part of security control assessments, [FedRAMP Assignment: at least annually], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing; [Assignment: organization-defined other forms of security assessment]].

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

Requirement: To include 'announced', 'vulnerability scanning’ to occur at least annually.

| **CA-2 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-2 (2)-1: at least annually | |
| Parameter CA-2 (2)-2: announced vulnerability scanning to occur at least annually | |
| Parameter CA-2 (2)-3: vulnerability scanning | |
| Parameter CA-2 (2)-4: as requested organization-defined other forms of security assessment | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| The GDIT Cloud includes as part of security control assessments at least annually, an announced vulnerability scanning to be conducted by a FedRAMP PMO approved 3PAO. The 3PAO includes this scanning as an assessment goal of the Security Assessment Plan prior to its approval by the FedRAMP PMO. GDIT and the 3PAO schedule the assessment, including these scans, in accordance with the FedRAMP PMO schedule for annual accreditation, marked by the anniversary of the initial P-ATO. |

#### CA-2 (3) Control Enhancement (M) (H)

The organization accepts the results of an assessment of [FedRAMP Assignment: organization-defined information system] performed by [FedRAMP Assignment: any FedRAMP Accredited 3PAO] when the assessment meets [FedRAMP Assignment: the conditions of the JAB/AO in the FedRAMP Repository].

| **CA-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-2 (3)-1: the GDIT Cloud | |
| Parameter CA-2 (3)-2: 3PAO | |
| Parameter CA-2 (3)-3: the conditions of an Agency ATO in the FedRAMP Secure Repository | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| We accept the results by working to remediate any deficiencies they state and adding those to our POA&M list. Our acceptance is validated by the JAB’s review. |

### 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** GDIT **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 | See section 10 for information about implementation details. |
| Part b | Click or tap here to enter text. |
| 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-3 (3) Control Enhancement (M) (H)

The organization prohibits the direct connection of an [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [FedRAMP Assignment: boundary protections which meet Trusted Internet Connection (TIC) requirements].

CA-3 (3) Additional FedRAMP Requirements and Guidance:

**Guidance:** Refer to Appendix H – Cloud Considerations of the TIC Reference Architecture document. Link: <https://www.dhs.gov/publication/tic-reference-architecture-22>

| **CA-3 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter CA-3 (3)-1: organization-defined unclassified, non-national security system | |
| Parameter CA-3 (3)-2: boundary protections which meet Trusted Internet Connections (TIC) requirements | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| GDIT prohibits the direct connection of this unclassified, non-national security system to an external network (GDIT-OC-POL-1 GDIT Cloud Security Policy, Section 4.4,). If a future FedRAMP control requires the direct connection to and external network, GDIT would require the use of appropriate Boundary Protection mechanism that meets Trusted Internet Connection (TIC) requirements. At this time there are no direct connections to an external network necessitating the use of a TIC. |

#### CA-3 (5) Control Enhancement (H)

The organization employs [FedRAMP Selection: deny-all, permit by exception] policy for allowing [FedRAMP Assignment: any systems] to connect to external information systems.

CA-3 (5) Additional FedRAMP Requirements and Guidance:

Guidance: For JAB Authorization, CSPs shall include details of this control in their architecture briefing.

| **CA-3 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter CA-3 (5)-1: deny-all, permit-by-exception | |
| Parameter CA-3 (5)-2: 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)  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 (5) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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 | Click or tap here to enter text. |
| Part b | 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 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 | 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 | Click or tap here to enter text. |
| 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 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: 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 | See CA-7 parts e, f, and g above for details on correlation and analysis, response actions, and status reporting. |
| Req. 2 | 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-7 (1) Control Enhancement (M) (H)

The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to monitor the security controls in the information system on an ongoing basis.

| **CA-7 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Owner | |
| Parameter CA-7 (1): complete independence | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| The Cloud System Owner ensures that a full independent assessment team is used to conduct assessments on an annual basis. The 3PAO is a FedRAMP requirement. The use of a 3PAO ensures the independence of the assessment team. See CA-2 parts a,b,c, and d for details on how the 3PAO conducts assessments. Day to day vulnerability management services are provided by GDIT employees from outside the management chain of the Information System Owner so as to ensure the assessment is provided without bias of operations management. |

#### CA-7 (3) Control Enhancement (H)

The organization employs trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.

| **CA-7 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### CA-8 Penetration Testing (M) (H)

The organization conducts penetration testing [FedRAMP Assignment: at least annually] on [Assignment: organization-defined information systems or system components].

CA-8 Additional FedRAMP Requirements and Guidance

Guidance: See the FedRAMP Documents page under Key Cloud Service

Provider (CSP) Documents> Penetration Test Guidance

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

| **CA-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter CA-8-1: at least annually | |
| Parameter CA-8-2: GDIT Cloud System | |
| 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-8 What is the solution and how is it implemented?** |
| --- |
| The 3PAO conducts penetration testing on the GDIT Cloud system in conjunction with the annual assessment. This activity is detailed in the Security Assessment Plan and reported in the Security Assessment Report, which is included as part of the GDIT Cloud authorization package. |

#### CA-8 (1) Control Enhancement (M) (H)

The organization employs an independent penetration agent or penetration team to perform penetration testing on the information system or system components.

| **CA-8 (1)** | **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 | |

| **CA-8 (1) What is the solution and how is it implemented?** |
| --- |
| GDIT employs an independent 3PAO to conduct penetration testing through the course of the annual security assessment. The 3PAO includes the details and extent of the independent penetration tests in the Security Assessment Plan (SAP). The SAP is reviewed and approved by the FedRAMP PMO and JAB before any testing is conducted. The results of these penetration tests are included in the 3PAO's Security Assessment Report (SAR) as required by the FedRAMP PMO. |

### 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 | Wireless access points (not applicable at this time) |
| Part b | 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 (H)

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 annually]; and
   2. Configuration management procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| **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 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 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?** |
| --- |
| See Section 9 for a list of hardware, software, and network baseline components. |

#### CM-2 (1) Control Enhancement (H)

The organization reviews and updates the baseline configuration of the information system:

1. [FedRAMP Assignment: at least annually or when a significant change occurs];
2. When required due to [FedRAMP Assignment: to include when directed by the JAB]; and
3. As an integral part of information system component installations and upgrades.

CM-2 (1) (a) Additional FedRAMP Requirements and Guidance:

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, Page F-7.

| **CM-2 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Configuration-Change Manager | |
| Parameter CM-2(1)(a): :Annually | |
| Parameter CM-2(1)(b): when directed 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 | |

| **CM-2 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Section 4.4 of the GDIT Cloud Service Asset and Configuration Management Process and Procedures Guide provides the details for the above activity. |
| Part b | The Configuration-Change Manager reviews and updates the baseline configuration when directed by the JAB. This process is the same as is described in part a of this control. |
| Part c | The Change Advisory Board (CAB) is responsible for the Configuration Management of the baseline and approving all changes, as defined in the GDIT Cloud Change Advisory Board (CAB) Procedures GuideGDIT Cloud Change Advisory Board (CAB) Procedures Guide. |

#### CM-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

| **CM-2 (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 (2) What is the solution and how is it implemented?** |
| --- |
| The spreadsheet has different tabs depending on what Configuration Item is being added/removed/updated in the CMDB. The tabs are VMs, Network Devices, Storage, Other CI. There are also two other tabs which provide an Overview and the valid cell values for specific fields. For example, the VM tab has: CI Action, Ticket Number, Friendly Name, HostName, Asset Status, Deployed Date, Retired Date, Compute Type, System Type, Primary Use, Site, Room/Grid, Long Description, Tenant, Program, FQDN, IP Address, Operating System, vCPUs, vRAM, vDisk, Disk Breakdown, SQL Server installed, # of SQL instances, SQL Version, Total # of SQL Cores, Owner by Team.Tripwire is the automated mechanism to review configuration settings to general business practices (e.g. DISA STIGs). |

#### CM-2 (3) Control Enhancement (H)

The organization retains [FedRAMP Assignment: the previously approved baseline configuration of IS components] to support rollback.

| **CM-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Configuration-Change Manager | |
| Parameter CM-2 (3): older than current baseline versions | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| All changes to a CI are saved within the individual CI record for the life of each CI. The Configuration-Change Manager documents the changes in the Journal tab of the Cherwell CMDB CI record for each CI. |

#### CM-2 (7) Control Enhancement (M) (H)

The organization:

1. Issues [Assignment: organization-defined information systems, system components, or devices] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and
2. Applies [Assignment: organization-defined security safeguards] to the devices when the individuals return.

| **CM-2 (7)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Configuration-Change Manager | |
| Parameter CM-2 (7)(a)-1: systems, system components, or devices | |
| Parameter CM-2 (7)(a)-2: None allowed | |
| Parameter CM-2 (7)(b): None allowed | |
| 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 (7) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | According to the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.5, GDIT Cloud mobile assets are not allowed to be taken to a high-risk location; specifically, any location outside the US. |
| Part b | Customer furnished laptops and other electronic devices are also restricted from travel if the device will connect to a GDIT network/infrastructure. In the event the device does not connect to a GDIT network, the decision to allow the device to travel to the restricted country lies with the customer. |

### CM-3 Configuration Change Control (M) (H)

The organization:

1. Determines the types of changes to the information system that are configuration-controlled;
2. Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses;
3. Documents configuration change decisions associated with the information system;
4. Implements approved configuration-controlled changes to the information system;
5. Retains records of configuration-controlled changes to the information system for [Assignment: organization-defined time period];

CM-3 (e) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with record retention policies and procedures.

1. Audits and reviews activities associated with configuration-controlled changes to the information system; and
2. Coordinates and provides oversight for configuration change control activities through [FedRAMP Assignment: see additional FedRAMP requirements and guidance] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined configuration change conditions]].

CM-3 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider establishes a central means of communicating major changes to or developments in the information system or environment of operations that may affect its services to the federal government and associated service consumers (e.g., electronic bulletin board, web status page). The means of communication are approved and accepted by the JAB/AO.

| **CM-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Configuration-Change Manager | |
| Parameter CM-3(e): 12 months | |
| Parameter CM-3(g)-1: through the Cherwell Ticketing System | |
| Parameter CM-3(g)-2: one or more | |
| Parameter CM-3(g)-3: times per week | |
| 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-3 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | as needed to review proposed changes |
| Part b | All change types require a ticket in the Cherwell system. |
| Part c | not in conflict with other planned changes |
| Part d | The Configuration-Change Manager documents all the change decisions in the GDIT Cloud Ticketing system (Cherwell) within a specific ticket number. The Cherwell ticket provides both an audit trail and a record of all changes and is retained in the ticket system for a minimum of 12 months to provide a historical reference for changes. |
| Part e | The GDIT Cloud engineers implement approved configuration-controlled changes to the system environment. The CR ticket is updated to include the deployment information, and the new configuration baseline is updated in the CMDB. |
| Part f | The Cherwell ticket provides both an audit trail and a record of all changes and is retained in the ticket system for a minimum of 12 months to provide a historical reference for changes. |
| Part g | All appropriate approvals received |

#### CM-3 (1) Control Enhancement (H)

The organization employs automated mechanisms to:

1. Document proposed changes to the information system;
2. Notify [Assignment: organization-defined configuration management approval authorities] of proposed changes to the information system and request change approval;
3. Highlight proposed changes to the information system that have not been approved or disapproved by [FedRAMP Assignment: organization agreed upon time period];
4. Prohibit changes to the information system until designated approvals are received;
5. Document all changes to the information system; and
6. Notify [FedRAMP Assignment: organization-defined configuration management approval authorities] when approved changes to the information system are completed.

| **CM-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: For a given change, the Implementer opens up the change, adds any notes to the Implementation Notes field, and the sends the notification email. This email goes to the GDIT Cloud Team and the affected Program’s distribution lists. At the end of the implementation, the Implementer updates the change record, provides specific notes in the Post Implementation field, and sends a Completion Notification to the same distribution lists. | |
| Parameter CM-3 (1)(b): Click or tap here to enter text. | |
| Parameter CM-3 (1)(c): Click or tap here to enter text. | |
| Parameter CM-3 (1)(f): Click or tap here to enter text. | |
| 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-3 (1) 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. |
| Part c | Click or tap here to enter text. |
| Part d | Click or tap here to enter text. |
| Part e | Click or tap here to enter text. |
| Part f | Click or tap here to enter text. |

#### CM-3 (2) Control Enhancement (M)(H)

The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

| **CM-3 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-3 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CM-3 (4) Enhancement (H)

The organization requires an information security representative to be a member of the [FedRAMP Assignment: configuration control board (CCB) or similar (as defined in CM-3)].

| **CM-3 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CM-3 (4): Click or tap here to enter text. | |
| 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-3 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CM-3 (6) Enhancement (H)

The organization ensures that cryptographic mechanisms used to provide [FedRAMP Assignment: all security safeguards that rely on cryptography] are under configuration management.

| **CM-3 (6)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CM-3 (6): Click or tap here to enter text. | |
| 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-3 (6) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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?** |
| --- |
| Click or tap here to enter text. |

#### CM-4 (1) Control Enhancement (H)

The organization analyzes changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

| **CM-4 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### CM-5 Access Restrictions for Change (M) (H)

The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

| **CM-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 | |

| **CM-5 What is the solution and how is it implemented?** |
| --- |
| Physical access to GDIT Cloud hardware for the purpose of conducting maintenance by an independent 3rd party resource requires a GDIT Cloud administrator escort. The access to perform changes in GDIT Cloud systems is strictly limited to the GDIT Cloud administrators of the affected devices. Visitors are required to show proof of identity. Each visitor is checked out at the end of work visit and visitor card is returned. Physical and logical access restrictions associated with changes to the information system are determined as part of the CAB review of the change request. |

#### CM-5 (1) Control Enhancement (M) (H)

The information system enforces access restrictions and supports auditing of the enforcement actions.

| **CM-5 (1)** | **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-5 (1) What is the solution and how is it implemented?** |
| --- |
| Security Analysts audit of the access restrictions enforcement actions through SIEM and Tripwire alerts. Tripwire monitors the system for changes and sends alerts to the Security Analysts to review and verify whether the changes were authorized or unauthorized. |

#### CM-5 (2) Control Enhancement (H)

The organization reviews information system changes [FedRAMP Assignment: at least every thirty (30) days] and [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.

| **CM-5 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CM-5 (2)-1: Click or tap here to enter text. | |
| Parameter CM-5 (2)-2: Click or tap here to enter text. | |
| 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-5 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CM-5 (3) Control Enhancement (M) (H)

The information system prevents the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

CM-5 (3) Additional FedRAMP Requirements and Guidance:

Guidance: If digital signatures/certificates are unavailable, alternative cryptographic integrity checks (hashes, self-signed certs, etc.) can be used.

| **CM-5 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Configuration Manager | |
| Parameter CM-5 (3): GDIT Cloud software and firmware components within the boundary | |
| 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-5 (3) What is the solution and how is it implemented?** |
| --- |
| For appliances, the respective administrator of each system obtains software updates directly from the vendors support portal requiring secure connections during all phases of the download process. |

#### CM-5 (5) Control Enhancement (M) (H)

The organization:

1. Limits privileges to change information system components and system-related information within a production or operational environment; and
2. Reviews and reevaluates privileges [FedRAMP Assignment: at least quarterly].

| **CM-5 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CM-5(5)(b)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 | |

| **CM-5 (5) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Components that are not linked to Active Directory (appliances) still require access to the environment using Active Directory before non-AD components can be accessed. Personnel are granted access to non-AD integrated devices (appliances) through the process described in AC-2. Privileged users on those devices are authorized to make changes as long as the changes have been approved as part of the established change management process. |
| Part b | The quarterly review is a secondary control to catch human errors in the access authorization process. |

### 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: 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 Authorization | |

| **CM-6 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | 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 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 authorized change process is documented in CM-3 . |
| Part d | Click or tap here to enter text. |

#### CM-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for [Assignment: organization-defined information system components].

| **CM-6 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter CM-6 (1): GDIT Cloud system components as listed in the control implementation | |
| 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-6 (1) What is the solution and how is it implemented?** |
| --- |
| Tripwire allows for central verification of configurations, however change management procedures require manual review before any maintenance is accomplished. |

#### CM-6 (2) Control Enhancement (H)

The organization employs [Assignment: organization-defined security safeguards] to respond to unauthorized changes to [Assignment: organization-defined configuration settings].

| **CM-6 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CM-6 (2)-1: Click or tap here to enter text. | |
| Parameter CM-6 (2)-2: Click or tap here to enter text. | |
| 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-6 (2) What is the solution and how is it implemented?** |
| --- |
| 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-7 (1) Control Enhancement (M) (H)

The organization:

1. Reviews the information system [FedRAMP Assignment: at least Monthly] to identify unnecessary and/or nonsecure functions, ports, protocols, and services; and
2. Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure].

| **CM-7 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter CM-7 (1)(a): at least Monthly | |
| Parameter CM-7 (1)(b): organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or nonsecure | |
| 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 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | The SOC generates a report to identify and track all access-lists that are captured for the firewall access-list review. The firewall access-list review report documents, in itemized form, all access-lists from the subject firewall(s) that have been designated for the firewall access-list review. The firewall access-list review report is distributed to the point of contact identified in this process. |
| Part b | The SOC Manager distributes the analysis and schedules a meeting to discuss the findings and plan remediation actions to be implemented under a Cherwell Request for Change. Once the RFC is opened, it is assigned to the Network Engineer who makes the change as indicated in the RFC. |

#### CM-7 (2) Control Enhancement (M) (H)

The information system prevents program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].

CM-7(2) Additional FedRAMP Requirements and Guidance:

Guidance: This control shall be implemented in a technical manner on the information system to only allow programs to run that adhere to the policy (i.e., white listing). This control is not to be based off of strictly written policy on what is allowed or not allowed to run.

| **CM-7 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter CM-7 (2): Ivanti Application Control | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| The Configuration-Change Manager authorizes the baseline that is maintained in the Cherwell CMDB under version control. The change management process identifies the process to change the baseline configuration, in the GDIT Cloud Change Management Process and Procedures Guide. |

#### CM-7 (5) Control Enhancement (H)

The organization:

1. Identifies [Assignment: organization-defined software programs authorized to execute on the information system];
2. Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and
3. Reviews and updates the list of authorized software programs [FedRAMP Assignment: at least quarterly or when there is a change].

| **CM-7 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CM-7 (5)(a): GDIT Cloud software programs authorized to execute on the information system as maintained in the CMDB | |
| Parameter CM-7 (5)(c): at least annually or when there is a change | |
| 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 (5) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | The System Manager identifies software programs authorized to execute on the GDIT Cloud through the processes and procedures identified in the GDIT Cloud Change Management Process and Procedures Guide. In addition, the Configuration-Change Manager authorizes the baseline that is maintained in the Cherwell CMDB under version control. The baseline includes both hardware and software that has been selected for operation in the system. Any changes to the list of selected software must undergo the processes and procedures named above. Any additional software is approved using the standard Change Management process. That is, an RFC is submitted and it is reviewed by the CMB and approved. Software licenses are part of the CMDB. |
| Part b | The System Manager employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system through Ivanti Application Control that operates at the kernel level. This allows the Ivanti agent to identify unapproved software before the attempt of execution and validate the software is signed by an approved vendor certificate. |
| Part c | On a quarterly basis, the Configuration Change Manager pulls the Application Control whitelist from the Ivanti application in order to conduct a review. The list is reviewed against the CMDB and is also compared against previous whitelist reviews. Each application is checked against the record of Cherwell service requests and requests for change to ensure each has been properly approved. The review is also conducted as needed when there is a change in the environment. |

### 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 | Click or tap here to enter text. |
| Part b | Click or tap here to enter text. |

#### CM-8 (1) Control Enhancement (M) (H)

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

Instruction: A description of the inventory information is documented in Section 10. It is not necessary to re-document it here.

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

| **CM-8 (1)** | **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-8 (1) What is the solution and how is it implemented?** |
| --- |
| Any change to the system (installation, removal, and update) requires a change request that is tracked in the Cherwell ticketing system. Once the change is approved and executed, the inventory baseline is also updated in the CMDB. |

#### CM-8 (2) Control Enhancement (H)

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

| **CM-8 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CM-8 (3) Control Enhancement (M) (H)

The organization:

1. Employs automated mechanisms [FedRAMP Assignment: Continuously, using automated mechanisms with a maximum five-minute delay in detection] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and
2. Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].

| **CM-8 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter CM-8 (3)(a): Continuously, using automated mechanisms with a maximum five-minute delay in detection | |
| Parameter CM-8 (3)(b): disables network access by such components; isolates the components; notifies 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-8 (3) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Ivanti Application Control operates at the kernel level. This allows the Ivanti agent to identify unapproved software before the attempt of execution and validate the software is signed by and approved vendor certificate. Ivanti employs a certificate signed software whitelisting to deny-by-default, approve-by-exception, the execution of installed components on Windows operating systems. |
| Part b | For Ivanti Application Control, if the agent detects unsigned or unapproved software the software is not permitted to execute. The Ivanti Manager then alerts SOC analysts of “rogue software” through the SIEM. In the case of Ivanti, the required actions of disabling network access and isolating the component(s) occur automatically along with providing a notification to SOC analysts. |

#### CM-8 (4) Control Enhancement (H)

The organization includes in the information system component inventory information, a means for identifying by [Selection (one or more): name; [FedRAMP Assignment: position and role]], individuals responsible/accountable for administering those components.

| **CM-8 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CM-8 (4): Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CM-8 (5) Control Enhancement (M) (H)

The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories.

| **CM-8 (5)** | **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-8 (5) What is the solution and how is it implemented?** |
| --- |
| Any discrepancies found are noted and validated with affected CI’s owned by Team. Any resulting changes to the CI are made to the affected CI record. A Cherwell Service Request or RFC is the request of record for the changes. The ticketwill track results, findings, and subsequent CMDB updates (changes/adds/deletes/decommissions). Any CI changes will be related to the approved RFC. |

### CM-9 Configuration Management Plan (M) (H)

The organization develops, documents, and implements a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and configuration management processes and procedures;
2. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
3. Defines the configuration items for the information system and places the configuration items under configuration management; and
4. Protects the configuration management plan for unauthorized disclosure and modification.

| **CM-9** | **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-9 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Configuration Management Processes and Procedures – Chapter 4 |
| Part b | The Configuration-Change Manager establishes a configuration baseline and reviews it annually. This baseline enables the IT infrastructure to be restored to a known configuration if a change or release fails. Baseline changes are monitored and controlled within the change management and configuration auditing functions described in CM-8(5). |
| Part c | All CI are placed under configuration management. |
| Part d | The Configuration-Change Manager stores the CMP on the secure GDIT Cloud SharePoint site and on the GDIT Cloud Cherwell system. Both systems are access controlled and are protected against unauthorized disclosure and modification. Access to both systems is governed by the process described in AC-2 parts c, d, e, and f. |

### 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 | 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 | Techservices utilizes Ivanti and Traverse to send email alerts prior to one month of license expiration. |
| Part c | 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-10 (1) Control Enhancement (M) (H)

The organization establishes the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].

| **CM-10 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CM-10 (1): HCSD-IT-POL-1.0, Free and Open Source Software Usage | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### CM-11 User-Installed Software (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 | 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 | Logs of software installations on both Windows and RHEL servers are recorded within the SIEM AlienVault. |

#### CM-11 (1) Control Enhancement (H)

The information system alerts [Assignment: organization-defined personnel or roles] when the unauthorized installation of software is detected.

| **CM-11 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CM-11 (1): Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

## Contingency Planning (CP)

### CP-1 Contingency Planning Policy and Procedures (H)

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 annually]; and
   2. Contingency planning procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| **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 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 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 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 | Alternate Customer Communication Lead |
| Part c | 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 | 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 | 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-2 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan development with organizational elements responsible for related plans.

| **CP-2 (1)** | **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 | |

| **CP-2 (1) What is the solution and how is it implemented?** |
| --- |
| In addition, coordination is performed with organizational elements, including the executive team, program management team, and FedRAMP ISSO. On an annual basis, the organizational entities meet to review each of the plans to determine if additional coordination activities are required due to Lessons Learned from previous activities and experiences, including training and testing exercises. |

#### CP-2 (2) Control Enhancement (M) (H)

The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

| **CP-2 (2)** | **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 | |

| **CP-2 (2) What is the solution and how is it implemented?** |
| --- |
| During the GDIT Cloud Engineering design meetings, capacity is reviewed across all Cloud nodes. Where required proactive steps are taken through the Acquisition and Change Management processes to add capacity in advance of requiring it. |

#### CP-2 (3) Control Enhancement (M) (H)

The organization plans for the resumption of essential missions and business functions within [Assignment: organization-defined time period] of contingency plan activation.

| **CP-2 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CP-2(3): the GDIT Cloud Recovery failover RTO | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| Further details for how GDIT has planned for the resumption of essential mission and business functions can be found in the GDIT Cloud IT Contingency Plan, v 3.2 (6/26/2017). |

#### CP-2 (4) Control Enhancement (H)

The organization plans for the resumption of all missions and business functions within [FedRAMP Assignment: time period defined in service provider and organization Service Level Agreement (SLA)] of contingency plan activation.

| **CP-2 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CP-2 (4): Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-2 (5) Control Enhancement (H)

The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

| **CP-2 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (5) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-2 (8) Control Enhancement (M) (H)

The organization identifies critical information system assets supporting essential missions and business functions.

| **CP-2 (8)** | **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 | |

| **CP-2 (8) What is the solution and how is it implemented?** |
| --- |
| Consequently, there is no tier component system recovery scheme, but rather a total restoration of all IaaS environment components at once in the process of failover from one data center to the other, which maintains an active-passive relationship. |

### 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?** |
| --- |
| 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-3 (1) Control Enhancement (H)

The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

| **CP-3 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

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

The organization:

1. Tests the contingency plan for the information system [FedRAMP Assignment: at least annually] using [FedRAMP Assignment: functional exercises] 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 | 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 | Click or tap here to enter text. |
| 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-4 (1) Control Enhancement (M) (H)

The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

| **CP-4 (1)** | **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-4 (1) What is the solution and how is it implemented?** |
| --- |
| Activation of the Contingency Plan is also a consideration for an Incident Response in isolating an affected aspect of the system. Members of the Contingency Plan Team listed in the CP also have roles and responsibilities delineated in the Incident Response Plan, GDIT Cloud Incident Response Plan. All activities regarding Incident Response and the Contingency Plan are communicated through the Operations Center. |

#### CP-4 (2) Control Enhancement (H)

The organization tests the contingency plan at the alternate processing site:

1. To familiarize contingency personnel with the facility and available resources; and
2. To evaluate the capabilities of the alternate processing site to support contingency operations.

| **CP-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (2) 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. |

### CP-6 Alternate Storage Site (M) (H)

The organization:

1. Establishes an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information; and
2. Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site.

| **CP-6** | **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 | |

| **CP-6 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | The GDIT Cloud alternate storage site is geographically distinct from the primary storage site. The alternate storage site maintains either redundant infrastructure that performs the same functions or duplicate copies of the virtual machines for all critical GDIT Cloud services in the event that the primary storage site is not available. Since both the primary and alternate storage sites for GDIT Cloud IaaS fall under the same authorization to operate (ATO), environmental conditions, access rules, physical and environmental protection requirements, and coordination of delivery/retrieval of backup media are included and described in this System Security Plan. Therefore, there is no need to establish agreements to permit the storage and recovery of information system backup information. The GDIT Cloud IaaS alternate storage site reflects the requirements in the contingency plan in order to maintain essential missions/business functions despite disruption, compromise, or failure in organizational information systems. |
| Part b | Secondary Site: The GDIT Cloud East - The Manassas data center is a federally-compliant, Tier III facility. |

#### CP-6 (1) Control Enhancement (M) (H)

The organization identifies an alternate storage site that is separated from the primary storage site to reduce susceptibility to the same threats.

| **CP-6 (1)** | **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 | |

| **CP-6 (1) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-6 (2) Control Enhancement (H)

The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

| **CP-6 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-6 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-6 (3) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| **CP-6 (3)** | **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 | |

| **CP-6 (3) What is the solution and how is it implemented?** |
| --- |
| Given the distance between the two, a catastrophic failure in one location would not affect the other. Virginia is low risk for Earthquakes and Tornados along with coastal flooding or damage by Hurricanes. Colorado has the opposite factors with Cold temperatures, possibility of Earthquakes and/or Tornados or snow storms. |

### CP-7 Alternate Processing Site (M) (H)

The organization:

1. Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined information system operations] for essential missions/business functions within [FedRAMP Assignment: see additional FedRAMP requirements and guidance] when the primary processing capabilities are unavailable;

CP-7a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

1. Ensures that equipment and supplies required to transfer and resume operations are available at the alternate processing site or contracts are in place to support delivery to the site within the organization-defined time period for transfer/resumption; and
2. Ensures that the alternate processing site provides information security safeguards equivalent to that of the primary site.

| **CP-7** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CP-7(a)-1: Full operations | |
| Parameter CP-7(a)-2: The GDIT Cloud defines a time period consistent with recovery time objectives as 24-48 hours. | |
| 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-7 What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Daily backups are transferred to the alternate data center daily, i.e., the GDIT Cloud Data Center West facility (Westminster, Colorado) is backup is transferred to the GDIT Cloud Data Center East facility (Manassas, Virginia) and vice versa. |
| Part b | The System Manager ensures that critical components of GDIT Cloud IaaS are present and available at the alternate processing site. With these components already in place and running at the alternate site, GDIT Cloud is able to conduct a failover to the alternate processing site within 48 hours as stated in the GDIT Cloud IT Contingency Plan. |
| Part c | Secondary Site: The GDIT Cloud East - The Manassas data center is a federally-compliant, Tier III facility. |

#### CP-7 (1) Control Enhancement (M) (H)

The organization identifies an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats.

CP-7(1) Additional FedRAMP Requirements and Guidance

Guidance: The service provider may determine what is considered a sufficient degree of separation between the primary and alternate processing sites, based on the types of threats that are of concern. For one particular type of threat (i.e., hostile cyber-attack), the degree of separation between sites will be less relevant.

| **CP-7 (1)** | **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 | |

| **CP-7 (1) What is the solution and how is it implemented?** |
| --- |
| Natural disasters affecting one site would not affect the other. Virginia is low risk for Earthquakes and Tornados along with coastal flooding or damage by Hurricanes. Colorado has the opposite with Cold temperatures, possibility of Earthquakes and/or Tornados or snow storms. |

#### CP-7 (2) Control Enhancement (M) (H)

The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

| **CP-7 (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 | |

| **CP-7 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-7 (3) Control Enhancement (M) (H)

The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives).

| **CP-7 (3)** | **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 | |

| **CP-7 (3) What is the solution and how is it implemented?** |
| --- |
| The Customer is responsible for developing alternate processing site agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives). |

#### CP-7 (4) Control Enhancement (H)

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential missions and business functions.

| **CP-7 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-7 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### CP-8 Telecommunications Services (M) (H)

The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of [Assignment: organization-defined information system operations] for essential missions and business functions within [FedRAMP Assignment: See CP-8 additional FedRAMP requirements and guidance] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

CP-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines a time period consistent with the recovery time objectives and business impact analysis.

| **CP-8** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter CP-8-1: Full operations | |
| Parameter CP-8-2: 45 seconds is the time period consistent with the business impact analysis | |
| 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-8 What is the solution and how is it implemented?** |
| --- |
| The System Manager has established that services failover services within 45 seconds of detection of an outage with one of the ISPs.This is performed through automated protocols configured in the network architecture. |

#### CP-8 (1) Control Enhancement (M) (H)

The organization:

1. Develops primary and alternate telecommunications service agreements that contain priority- of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and
2. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

| **CP-8 (1)** | **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 | |

| **CP-8 (1) What is the solution and how is it implemented?** | |
| --- | --- |
| Part a | Table 11-8. Redundant Telecommunication Service Providers |
| Part b | If a customer requires a TSP for GDIT Cloud circuits that support the customer’s role in National Security/Emergency Preparedness, GDIT will work with the customer to establish the TSP. |

#### CP-8 (2) Control Enhancement (M) (H)

The organization obtains alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

| **CP-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)  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-8 (2) What is the solution and how is it implemented?** |
| --- |
| All ISPs are under contractual SLA's and with the utilization of BGP protocols, The GDIT Cloud self-manages all routing and ISP selection within the blends. |

#### CP-8 (3) Control Enhancement (H)

The organization obtains alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

| **CP-8 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-8 (3) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-8 (4) Control Enhancement (H)

The organization:

1. Requires primary and alternate telecommunications service providers to have contingency plans;
2. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and
3. Obtains evidence of contingency testing/training by providers [FedRAMP Assignment: annually].

| **CP-8 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CP-8 (4)(c): Click or tap here to enter text. | |
| 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-8 (4) 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. |
| Part c | Click or tap here to enter text. |

### 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 | Click or tap here to enter text. |
| Part b | The backup storage capability is approved and accepted by the JAB. |
| Part c | 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-9 (1) Control Enhancement (H)

The organization tests backup information [FedRAMP Assignment: at least monthly] to verify media reliability and information integrity.

| **CP-9 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Contingency Plan Director | |
| Parameter CP-9 (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)  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 (1) What is the solution and how is it implemented?** |
| --- |
| The Contingency Plan Director tests backups annually to verify media reliability and information integrity as part of annual CP testing. The GDIT Cloud IT Contingency Plan requires testing using a scenario where a restoration of backup data is tested. |

#### CP-9 (2) Control Enhancement (H)

The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.

| **CP-9 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

#### CP-9 (3) Control Enhancement (M) (H)

The organization stores backup copies of [Assignment: organization-defined critical information system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.

| **CP-9 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter CP-9 (3): Full system backup | |
| 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 (3) What is the solution and how is it implemented?** |
| --- |
| The GDIT Cloud inventory (including hardware, software, and firmware components) is stored in the GDIT Cloud CMDB. |

#### CP-9 (5) Control Enhancement (H)

The organization transfers information system backup information to the alternate storage site [FedRAMP Assignment: time period and transfer rate consistent with the recovery time and recovery point objectives defined in the service provider and organization SLA].

| **CP-9 (5)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CP-9 (5): Click or tap here to enter text. | |
| 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 (5) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

### 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?** |
| --- |
| 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. |

#### CP-10 (2) Control Enhancement (M) (H)

The information system implements transaction recovery for systems that are transaction-based.

| **CP-10 (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 | |

| **CP-10 (2) What is the solution and how is it implemented?** |
| --- |
| If Customer has a transaction-based system, then the customer is responsible for considering how to implement transaction recovery for Customer systems that are transaction-based. |

#### CP-10 (4) Control Enhancement (H)

The organization provides the capability to restore information system components within [FedRAMP Assignment: time period consistent with the restoration time-periods defined in the service provider and organization SLA] from configuration-controlled and integrity-protected information representing a known, operational state for the components.

| **CP-10 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter CP-10 (4): Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented?** |
| --- |
| Click or tap here to enter text. |

## Identification and Authentication (IA)

### IA-1 Identification and Authentication Policy and Procedures (H)

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

(b) Reviews and updates the current:

* 1. Identification and authentication policy [FedRAMP Assignment: at least annually]; and
  2. Identification and authentication procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| **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 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 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? |
| --- |
| Click or tap here to enter text. |

#### 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? |
| --- |
| 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 (2) Control Enhancement (M) (H)

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

| **IA-2 (2)** | **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 (2) What is the solution and how is it implemented? |
| --- |
| 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 (3) Control Enhancement (M) (H)

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

| **IA-2 (3)** | **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 (3) What is the solution and how is it implemented? |
| --- |
| An exception can be made by submitting a ticket to the Cherwell system when a token is lost. This action requires approval by the Security Operations Manager or ISSO before modifying the system to allow a user to log in to his or her laptop with single-factor authentication. Once the user receives a new token, the system is reverted back to enable multi-factor authentication for local access and the approving authority (Security Operations Manager or ISSO) is informed via email. |

#### IA-2 (4) Control Enhancement (H)

The information system implements multifactor authentication for local access to non-privileged accounts.

| **IA-2 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IA-2 (5) Control Enhancement (M) (H)

The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

| **IA-2 (5)** | **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-2 (5) What is the solution and how is it implemented? |
| --- |
| Group authenticators are not used in the GDIT Cloud IaaS. Individuals must authenticate using their own credentials. The only time a person can access an account apart from an individual account is in the event of an emergency, break-glass situation where the password is shared but controlled through SOP and Password Manager Pro. Strictly speaking, this is not a group authenticator. |

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

The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.

| **IA-2 (8)** | **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 (8) What is the solution and how is it implemented? |
| --- |
| See Section 9.4.4 Remote Access Data Flow for more information about the RSA solution. |

#### IA-2 (9) Control Enhancement (H)

The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

| **IA-2 (9)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (9) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IA-2 (11) Control Enhancement (M) (H)

The information system implements multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [FedRAMP Assignment: FIPS 140-2, NIAP\* Certification, or NSA approval].

\*National Information Assurance Partnership (NIAP)

Additional FedRAMP Requirements and Guidance:

Guidance: PIV = separate device. Please refer to NIST SP 800-157 Guidelines for Derived Personal Identity Verification (PIV) Credentials. FIPS 140-2 means validated by the Cryptographic Module Validation Program (CMVP).

| **IA-2 (11)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-2 (11): RSA system employs a combination of a user-defined PIN and a Passcode that changes every 60 seconds | |
| 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 (11) What is the solution and how is it implemented? |
| --- |
| A passcode provided by the RSA SecureID hard token that is a separate device. |

#### 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? |
| --- |
| 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-3 Device Identification and Authentication (M) (H)

The information system uniquely identifies and authenticates [Assignment: organization-defined specific and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

| **IA-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter IA-3-1: Specific devices and/or types of devices: | |
| Parameter IA-3-2: network | |
| 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-3 What is the solution and how is it implemented? |
| --- |
| Systems which have not previously been identified, or “rogue assets,” are detected in accordance with control CM-8(3) Automated Unauthorized Component Detection, by the AlienVault SIEM and an alert generated to Security Analysts for further investigation and incident response. |

### IA-4 Identifier Management (H)

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

1. Receiving authorization from [FedRAMP Assignment at a minimum, the ISSO (or similar role within the organization)] 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: thirty-five (35) days (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 | 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 | Example: s-sqleng (service account for the SQL engine) |
| Part c | 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 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 | 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-4 (4) Control Enhancement (M) (H)

The organization manages individual identifiers by uniquely identifying each individual as [FedRAMP Assignment: contractors; foreign nationals].

| **IA-4 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: HR | |
| Parameter IA-4 (4): contractors; foreign nationals | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### IA-5 Authenticator Management (H)

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 3. Link <https://pages.nist.gov/800-63-3>

| **IA-5** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-5(g60 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 | 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 | 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 | 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 | A user is terminated from the system. Procedures outlined for AC-2 are followed in this case. |
| Part e | The Engineer responsible for the respective system ensures the appropriate hardening guidelines are followed and that default authenticators are changed. |
| Part f | Passwords may not be reused for 24 generations |
| Part g | 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 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 | Devices are configured to do hashing functions and encryption as described in part h above. |
| Part j | 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 (H)

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 fifty percent (50%)];
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 | 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 | 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 | 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 | 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 | 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 | 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 (2) Control Enhancement (M) (H)

The information system, for PKI-based authentication:

1. Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information;
2. Enforces authorized access to the corresponding private key;
3. Maps the authenticated identity to the account of the individual or group; and
4. Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

| **IA-5 (2)** | **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-5 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud solution certificates are signed by a trusted, internal certificate authority (CA). When issued from the internal certificate authority, each certificate includes the full certification patch to include the certificate for the issuing CA. |
| Part b | Only GDIT Cloud administrators can generate and manage certificates from the GDIT Cloud trusted certificate authority. |
| Part c | The GDIT Cloud certificate authorities do not issue certificates for user authentication. RSA Multifactor Authentication is being used as an alternative user authentication method. |
| Part d | The GDIT Cloud implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network. |

#### IA-5 (3) Control Enhancement (M) (H)

The organization requires that the registration process to receive [FedRAMP Assignment: All hardware/biometric (multifactor authenticators] be conducted [FedRAMP Selection: in person] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].

| **IA-5 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-5 (3)-1: All hardware/biometric multifactor authenticators | |
| Parameter IA-5 (3)-2: in person | |
| Parameter IA-5 (3)-3: RSA tokens | |
| Parameter IA-5 (3)-4: 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-5 (3) What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud solution does not use smart cards in the Platform environment; rather, it uses RSA tokens that are distributed by a designated authority in conformance with GDIT Cloud Employee On-Boarding and Off-Boarding. |

#### IA-5 (4) Control Enhancement (H)

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy [FedRAMP Assignment: complexity as identified in IA-5 (1) Control Enhancement (H) Part A].

IA-5(4) Additional FedRAMP Requirements and Guidance:

Guidance: If automated mechanisms which enforce password authenticator strength at creation are not used, automated mechanisms must be used to audit strength of created password authenticators.

| **IA-5 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IA-5(4using an approved tool with characteristics of 15 character length with complexity requirements) | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud default Administrator passwords are cleared at time of solution installation and then stored in the safe described in IA-2 (3). |

#### IA-5 (6) Control Enhancement (M) (H)

The organization protects authenticators commensurate with the security category of the information to which use of the authenticator permits access.

| **IA-5 (6)** | **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-5 (6) What is the solution and how is it implemented? |
| --- |
| Further, Customers are responsible for ensuring that critical information, such as privileged credentials, be encrypted in transit and at rest, and that they define requirements for access, access control, and access logging when utilizing their own multifactor authentication mechanism within their Virtual Machines and supported applications. |

#### IA-5 (7) Control Enhancement (M) (H)

The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

| **IA-5 (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-5 (7) What is the solution and how is it implemented? |
| --- |
| All GDIT Cloud systems credentials are encrypted by the COTS applications or stored in an encrypted storage volume. |

#### IA-5 (8) Control Enhancement (H)

The organization implements [FedRAMP Assignment: different authenticators on different systems] to manage the risk of compromise due to individuals having accounts on multiple information systems.

| **IA-5 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter IA-5 (8Click or tap here to enter text.) | |
| 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 (8) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### 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 (11separate 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? |
| --- |
| Click or tap here to enter text. |

#### IA-5 (13) Control Enhancement (H)

The information system prohibits the use of cached authenticators after [Assignment: organization-defined time period].

| **IA-5 (13)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter IA-5 (13Click or tap here to enter text.) | |
| 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 (13) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| 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? |
| --- |
| 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)  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 (1) What is the solution and how is it implemented? |
| --- |
| 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)  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 (2) What is the solution and how is it implemented? |
| --- |
| 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 (3GDIT 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)  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 (3) What is the solution and how is it implemented? |
| --- |
| 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)  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 (4) What is the solution and how is it implemented? |
| --- |
| 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 (H)

The organization:

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

| **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 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 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 (H)

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 [FedRAMP Assignment: ten (10) days] 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 | 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 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 annual training is included on the Security Calendar that contains the continuous monitoring FedRAMP requirements. |

#### IR-2 (1) Control Enhancement (H)

The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

| **IR-2 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IR-2 (2) Control Enhancement (H)

The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment.

| **IR-2 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### IR-3 Incident Response Testing (H)

The organization tests the incident response capability for the information system [FedRAMP Assignment: at least every six (6) months] using [FedRAMP Assignment: see additional FedRAMP Requirements and Guidance] to determine the incident response effectiveness and documents the results.

IR-3 Additional FedRAMP Requirements and Guidance:

Requirements: The service provider defines tests and/or exercises in accordance with NIST Special Publication 800-61 (as amended). For JAB authorization, the service provider provides test plans to the JAB/AO annually. Test plans are approved and accepted by the JAB/AO prior to the test commencing.

| **IR-3** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Security Operations Manager | |
| Parameter IR-3-1: at least annually | |
| Parameter IR-3-2: Test plans are approved and accepted by the AO prior to the test commencing | |
| 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-3 What is the solution and how is it implemented? |
| --- |
| The 2017 IT Test was performed on 5/24/2017. |

#### IR-3 (2) Control Enhancement (M) (H)

The organization coordinates incident response testing with organizational elements responsible for related plans.

| **IR-3 (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 | |

| IR-3 (2) What is the solution and how is it implemented? |
| --- |
| For instance, incident response (handling) is included within the contingency plan testing. Incident response testing is conducted within the Contingency Plan Table Top exercise. |

### 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 | Click or tap here to enter text. |
| Part b | 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 GDIT Cloud ISSO, (in conjunction with Customer ISSO), reviews the Security Incident Report and conducts Lessons Learned exercises based on incident reports. |

#### IR-4 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to support the incident handling process.

| **IR-4 (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 | |

| IR-4 (1) What is the solution and how is it implemented? |
| --- |
| The Security Operations Manager employs automated mechanisms to support the incident handling process Security incidents are tracked via GDIT Cloud MSS ticketing system (Cherwell). . |

#### IR-4 (2) Control Enhancement (H)

The organization includes dynamic reconfiguration of [FedRAMP Assignment: all network, data storage, and computing devices] as part of the incident response capability.

| **IR-4 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter IR-4 (2): Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IR-4 (3) Control Enhancement (H)

The organization identifies [Assignment: organization-defined classes of incidents] and [Assignment: organization-defined actions to take in response to classes of incident] to ensure continuation of organizational missions and business functions.

| **IR-4 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter IR-4 (3)-Click or tap here to enter text.1 | |
| Parameter IR-4 (3)-2: Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IR-4 (4) Control Enhancement (H)

The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

| **IR-4 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IR-4 (6) Control Enhancement (H)

The organization implements incident handling capability for insider threats.

| **IR-4 (6)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (6) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IR-4 (8) Control Enhancement (H)

The organization implements incident handling capability for insider threats.

The organization coordinates with [FedRAMP Assignment: external organizations including consumer incident responders and network defenders and the appropriate consumer incident response team (CIRT)/ Computer Emergency Response Team (CERT) (such as US-CERT, DoD CERT, IC CERT)] to correlate and share [Assignment: organization-defined incident information] to achieve a cross- organization perspective on incident awareness and more effective incident responses.

| **IR-4 (8)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter IR-4 (8)-1: Click or tap here to enter text. | |
| Parameter IR-4 (8)-2: Click or tap here to enter text. | |
| 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 (8) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| Upon resolution, GDIT Cloud security team generates a post mortem After Action Report with root cause analysis. See GDIT Cloud Incident Response Plan ). |

#### IR-5 (1) Control Enhancement (H)

The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

| **IR-5 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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 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 | Click or tap here to enter text. |

#### IR-6 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to assist in the reporting of security incidents.

| **IR-6 (1)** | **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-6 (1) What is the solution and how is it implemented? |
| --- |
| In addition to GDIT Cloud Border Guard IDS to monitor intrusions we leverage the GDIT Cloud MMS SIEM. The GDIT Cloud MMS SIEM receives syslog streams from all devices that we monitor including the devices in the GDIT Cloud IaaS. The GDIT Cloud MMS SIEM leverages syslog correlation capabilities to generate alerts regarding security, performance and other anomalies, which assists in the reporting of security incidents. |

### 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? |
| --- |
| 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-7 (1) Control Enhancement (M) (H)

The organization employs automated mechanisms to increase the availability of incident response related information and support.

| **IR-7 (1)** | **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-7 (1) What is the solution and how is it implemented? |
| --- |
| In the event of a security incident, GDIT Cloud operations will take ownership of the incident and notify the GDIT Cloud Information Security team to investigate and remediate. Upon resolution, the GDIT Cloud Information Security team will generate a post mortem incident report with root cause analysis. This root cause will be provided to the appropriate parties identified in the GDIT Cloud Incident Response Plan. |

#### IR-7 (2) Control Enhancement (M) (H)

The organization:

1. Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
2. Identifies organizational incident response team members to the external providers.

| **IR-7 (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 | |

| IR-7 (2) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Customers are responsible to establish a direct, cooperative relationship between its incident response capability and external providers of information system protection capability. |
| Part b | Customers are responsible to identify organizational incident response team members to the external providers. |

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

The organization:

1. Develops an incident response plan that:
2. Provides the organization with a roadmap for implementing its incident response capability;
3. Describes the structure and organization of the incident response capability;
4. Provides a high-level approach for how the incident response capability fits into the overall organization;
5. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
6. Defines reportable incidents;
7. Provides metrics for measuring the incident response capability within the organization;
8. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
9. Is reviewed and approved by [Assignment: organization-defined personnel or roles];
10. 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 | (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 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 | 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 | System/organizational changes or problems encountered during plan implementation, execution, or testing |
| Part e | 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. |

### IR-9 Information Spillage Response (M) (H)

The organization responds to information spills by:

1. Identifying the specific information involved in the information system contamination;
2. Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
3. Isolating the contaminated information system or system component;
4. Eradicating the information from the contaminated information system or component;
5. Identifying other information systems or system components that may have been subsequently contaminated; and
6. Performing other [Assignment: organization-defined actions].

| **IR-9** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IR Team | |
| Parameter IR-9(b): Director, Data Center Operations, Manager, Engineering Services, ISSO | |
| Parameter IR-9(f): Post-incident activities | |
| 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-9 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Click or tap here to enter text. |
| Part b | The GDIT Cloud Incident Response team responds to information spills by alerting the Director, Data Center Operations, System Manager, and the ISSO utilizing the Security Incident Notification procedure, KA 10725 Security Incident Notification Checklist, that uses a method of communication not associated with the spill. In other words, if an email server were to be compromised, personnel would not send alerts using that email server. The notification is sent from GDIT email, not from email within the GDIT Cloud. |
| Part c | Click or tap here to enter text. |
| Part d | Click or tap here to enter text. |
| Part e | Click or tap here to enter text. |
| Part f | Click or tap here to enter text. |

#### IR-9 (1) Control Enhancement (M) (H)

The organization assigns [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills.

| **IR-9 (1)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter IR-9 (1): IR Team | |
| 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-9 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### IR-9 (2) Control Enhancement (H)

The organization provides information spillage response training [FedRAMP Assignment: at least annually].

| **IR-9 (2)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter IR-9 (2): 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-9 (2) What is the solution and how is it implemented? |
| --- |
| Training sign in sheets and individual Completion Certificates are saved in the secure GDIT Cloud SharePoint site, along with our training tracker. Training materials (brown bag slide decks) are saved in the “Training” shared folder in techservices that are accessed via the GDIT Cloud workstations. |

#### IR-9 (3) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined procedures] to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.

| **IR-9 (3)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: IR Team | |
| Parameter IR-9 (3): Data Spillage Checklist, KA 11397, SOP: Information Spillage Checklist | |
| 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-9 (3) What is the solution and how is it implemented? |
| --- |
| Once the “clear” systems have been identified, all personnel not involved in the corrective actions continue their tasks as assigned. As part of spillage training, personnel are to report any experienced impacts to the SOC Manager who then directs efforts to the affected asset to ensure minimal impact to assigned task accomplishment. |

#### IR-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] for personnel exposed to information not within assigned access authorizations.

| **IR-9 (4)** | **Control Summary Information** |
| --- | --- |
| Responsible Role: HR | |
| Parameter IR-9 (4): Non-disclosure agreement | |
| 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-9 (4) What is the solution and how is it implemented? |
| --- |
| In the event that personnel are exposed to information not within assigned access authorizations, the SOC Manager contacts the HR Department who follows up by contacting the individuals exposed and reviewing the requirements outlined in the NDA. Following the discussion, the individuals exposed are required to sign the NDA. |

## Maintenance (MA)

### MA-1 System Maintenance Policy and Procedures (H)

The organization:

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

| 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 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 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 | List of equipment removed or replaced (including identification numbers, if applicable) |
| Part b | 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 | 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 | List of equipment removed or replaced (including identification numbers, if applicable in organizational maintenance records. |

#### MA-2 (2) Control Enhancement (H)

The organization:

1. Employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and
2. Produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed.

| MA-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (2) 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. |

### MA-3 Maintenance Tools (M) (H)

The organization approves, controls, and monitors information system maintenance tools.

| MA-3 | 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 | |

| MA-3 What is the solution and how is it implemented? |
| --- |
| Installations/deployments of tools to the Cloud environment is monitored via the GDIT Cloud’s SIEM solution by the Security Analyst. Hardware-based tools brought into the data center (e.g., network tap, etc.) must be inspected by the field security officer and the escort for obvious modifications. The Engineer/escort indicates the tool has been inspected by filling out the maintenance sign-in sheet in the data center (see MA-3(1) below). The Engineer monitors the deployment/installation of the maintenance tool and observes it being used. If the tool is needed for an extended period of time (i.e., for more than the duration of the visit to the data center), it may remain deployed for the stated duration. |

#### MA-3 (1) Control Enhancement (M) (H)

The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

| MA-3 (1) | 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-3 (1) What is the solution and how is it implemented? |
| --- |
| When a 3rd party auditor applies software tools to examine known risks associated with the GDIT Cloud components (switches, servers, routers, firewalls), the results from these tools are reviewed for GDIT Cloud data. |

#### MA-3 (2) Control Enhancement (M) (H)

The organization checks media containing diagnostic and test programs for malicious code before the media are used in the information system.

| MA-3 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| 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-3 (2) What is the solution and how is it implemented? |
| --- |
| All media is scanned for viruses and their checksums are verified with those from the vendor, if available. . Symantec Endpoint Protection is configured to scan all files on a system including new media as it is inserted into the system prior to user access. |

#### MA-3 (3) Control Enhancement (M) (H)

The organization prevents the unauthorized removal of maintenance equipment containing organizational information by:

1. Verifying that there is no organizational information contained on the equipment;
2. Sanitizing or destroying the equipment;
3. Retaining the equipment within the facility; or
4. Obtaining an exemption from [FedRAMP Assignment: the information owner explicitly authorizes removal of the equipment from the facility].

| MA-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MA-3(3)(d): System Owner | |
| 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-3 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud prevents the unauthorized removal of maintenance equipment and/or the information which may be contained on maintenance equipment through the physical and technical (booting up and reviewing embedded memory on devices) inspection of devices which contain nonvolatile memory or are used to profile equipment or network elements within or associated with the data center. |
| Part b | The GDIT Cloud prevents the unauthorized removal of maintenance equipment and/or the information which may be contained on maintenance equipment through removing and sanitizing removable memory or using built in erase/reset capability for devices which, do not have removable memory but, may contain data center information. |
| Part c | GDIT Cloud retains all of the maintenance equipment within the Cloud facility. Any personnel or vendors performing any maintenance are only allowed to bring tools that do not store information, such as hammers and ratchets. |
| Part d | The GDIT Cloud prevents the unauthorized removal of maintenance equipment and/or the information which may be contained on maintenance equipment by maintaining equipment used for maintenance purposes within the facility and in a designated and locked cabinet.by obtaining an exemption from the system owner explicitly authorizing removal of the equipment from the facility. |

### 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 | 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-4 (2) Control Enhancement (M) (H)

The organization documents in the security plan for the information system, the policies and procedures for the establishment and use of nonlocal maintenance and diagnostic connections.

| MA-4 (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 | |

| MA-4 (2) What is the solution and how is it implemented? |
| --- |
| Non-local maintenance is not a desired method of maintenance or troubleshooting. It is only used when absolutely necessary. Details of these sessions are documented in the CR, AAR, or Lessons Learned document. Afterwards, the technical details will be presented to technical CAB members so they are aware of the circumstances that led to vendor support being needed. This ensures the same mistakes are not made multiple times and increases overall stability of GDIT Cloud. |

#### MA-4 (3) Control Enhancement (H)

The organization:

1. Requires that nonlocal maintenance and diagnostic services be performed from an information system that implements a security capability comparable to the capability implemented on the system being serviced; or
2. Removes the component to be serviced from the information system prior to nonlocal maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software) before reconnecting the component to the information system.

| MA-4 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (3) 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. |

#### MA-4 (6) Enhancement (H)

The information system implements cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications.

| MA-4 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (6) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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 | Authorized Vendor Personnel list |
| Part c | 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. |

#### MA-5 (1) Control Enhancement (H)

The organization:

1. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
   1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;
   2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
2. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

| MA-5 (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)  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 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | When maintenance personnel do not have the necessary access authorizations, GDIT Cloud personnel with the appropriate access authorizations escorts and supervises maintenance personnel AT ALL TIMES during the performance of maintenance activities on the information system in accordance with the GDIT Cloud Physical and Personnel policy. |
| Part b | Only MA-5 (1)(a)(1) is required by FedRAMP Moderate Baseline. |

### MA-6 Timely Maintenance (M) (H)

The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure.

| MA-6 | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter MA-6(1): The system owner must identify and maintain a list of security-critical information system components and/or key information technology components, as follows:; ; Cisco network equipment; Cisco UCS chassis; NetApp storage (drives) | |
| Parameter MA-6(2): Spare parts must be obtained for key components of the information system within 4 hours of component failure. Maintenance support for the components must be obtained within 48 hours of component failure. | |
| 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-6 What is the solution and how is it implemented? |
| --- |
| Customers are responsible for obtaining maintenance support and/or spare parts for components in their environment within a specific time period and for requesting the appropriate level of high availability, contingency response, or disaster recovery options as provided by the GDIT Cloud. |

## Media Protection (MP)

### MP-1 Media Protection Policy and Procedures (H)

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:
   1. Media protection policy [FedRAMP Assignment: at least annually]; and
   2. Media protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 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 (H)

The organization restricts access to [FedRAMP Assignment: any digital and non-digital media deemed sensitive] 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? |
| --- |
| 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-3 Media Labeling (M) (H)

The organization:

1. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
2. Exempts [FedRAMP Assignment: no removable media types] from marking as long as the media remain within [Assignment: organization-defined controlled areas].

MP-3(b) Additional FedRAMP Requirements and Guidance:

Guidance: Second parameter in MP-3(b)-2 is not applicable.

| MP-3 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MP-3(b)-1: no removable media types | |
| Parameter MP-3(b)-2: Not applicablnot applicablee | |
| 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-3 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Though these hard drives are FIPS 140-2 Level 3 validated, the SOC does not process PII, PCI, PHA, or Classified Information of any kind. The markings are for asset inventory only and do not indicate the distribution handling or caveats. |
| Part b | According to the GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.9, the ISSO does not allow any types of media or hardwarecomponents within the GDIT Cloud facilities to be removed without labeling described in part a; therefore, there are no exemptions from media marking for any type of removable media. |

### MP-4 Media Storage (M) (H)

The organization:

1. Physically controls and securely stores [FedRAMP Assignment: [all types of digital and non-digital media with sensitive information]] within [FedRAMP Assignment: see additional FedRAMP requirements and guidance]; and

MP-4a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines controlled areas within facilities where the information and information system reside.

1. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

| MP-4 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MP-4(a)-1: all types of digital and non-digital media with sensitive information | |
| Parameter MP-4(a)-2: controlled areas within facilities where the information and information system reside | |
| 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-4 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The removable media uses FIPS 140-2 encryption to protect the data contained on the media. |
| Part b | KA10723 - How To: Handling Requirements for External Portable Drives, KA10666 - GDIT Cloud Chain of Custody Form,KA 10668 - Approved Removable Media Check-out SOP and Inventory KA 10693 - How To: Request USB Storage |

### MP-5 Media Transport (M) (H)

The organization:

1. Protects and controls [FedRAMP Assignment: all media with sensitive information] during transport outside of controlled areas using [FedRAMP Assignment: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container];

MP-5a Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines security measures to protect digital and non-digital media in transport. The security measures are approved and accepted by the JAB/AO.

1. Maintains accountability for information system media during transport outside of controlled areas;
2. Documents activities associated with the transport of information system media; and
3. Restricts the activities associated with transport of information system media to authorized personnel.

| MP-5 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter MP-5(a)-1: all media with sensitive information | |
| Parameter MP-5(a)-2: for digital media, encryption using a FIPS 140-2 validated encryption module; for non-digital media, secured in locked container | |
| 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-5 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | KA10723 - How To: Handling Requirements for External Portable Drives, retained in the Cherwell repository provides the detailed steps and handling requirements by limiting the access of the drives to GDIT Cloud authorized individuals identified by name in KA 10667, Approved Media Transport Personnel while in an unencrypted mode. When disconnected from the information system, the removable media automatically encrypts the data, allowing for secure transportation by individuals other than those identified. A KA 10666, Chain of Custody Form, is included with the removable media while out of the controlled area and inspected by the SOC Analyst upon its return to the data center, before sanitization in accordance with KA 10992 Cloud Media Sanitization Procedure. |
| Part b | The System Manager maintains accountability for information system media during transport outside of GDIT Cloud Data Center areas with the “GDIT Cloud Chain Of Custody” document and the process described in the KA10723 - How To: Handling Requirements for External Portable Drives in conjunction with KA10666 - GDIT cloud Chain of Custody Form. |
| Part c | The GDIT Cloud personnel who transport information system media document activities associated with the transport in the KA10666 - GDIT cloud Chain of Custody Form. |
| Part d | Training consists of a demonstration of the successful understanding of the transport process found in Knowledge Article KA10723 - How To: Handling Requirements for External Portable Drives and associated KAs. This document resides in the Cherwell repository and provides the detailed steps and handling requirements by limiting the access of the drives to GDIT Cloud authorized individuals and Customer or the Customer system representative for their Customer external information systems. This includes a Chain of Custody form. |

#### MP-5 (4) Control Enhancement (M) (H)

The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

| MP-5 (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 | |

| MP-5 (4) What is the solution and how is it implemented? |
| --- |
| The Customer is responsible for employing cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. |

### MP-6 Media Sanitization and Disposal (H)

The organization:

1. Sanitizes [*Assignment: organization-defined information system media]* prior to disposal, release out of organizational control, or release for reuse using *[FedRAMP Assignment: techniques and procedures IAW NIST SP 800-88 R1, Appendix A - Minimum Sanitization Recommendations* ] 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 | Click or tap here to enter text. |
| Part b | 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-6 (1) Control Enhancement (H)

The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

| MP-6 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### MP-6 (2) Control Enhancement (H)

The organization tests sanitization equipment and procedures [FedRAMP Assignment: at least every six (6) months] to verify that the intended sanitization is being achieved.

MP-6(2) Additional FedRAMP Requirements and Guidance:

Guidance: Equipment and procedures may be tested or evaluated for effectiveness.

| MP-6 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter MP-6(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 | |

| MP-6 (2) What is the solution and how is it implemented? |
| --- |
| Applied Magnetics Laboratory AML-6KG Degaussing Wand is a GSA approved tool listed on the NSA Evaluated Products List used to sanitize hard disk drives or any other magnetic media if they cannot be wiped using BC Wipe. This device is a hand held permanent magnet degaussers. 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-6 (3) Control Enhancement (H)

The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].

| MP-6 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter MP-6 (3): Click or tap here to enter text. | |
| 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 (3) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| 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. |

#### MP-7 (1) Control Enhancement (M) (H)

The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

| MP-7 (1) | 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 | |

| MP-7 (1) is the solution and how is it implemented? |
| --- |
| Per GDIT-OC-POL-1, GDIT Cloud Security Policy, Section 4.1 (Access Control), all devices in the GDIT Cloud are associated with an identifiable owner. Consequently, the System Manager prohibits the use of portable storage devices in the GDIT Cloud when such devices have no identifiable owner. 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. Additionally, approved media for use in GDIT Cloud must be marked in accordance with the description provided in MP-3. |

## Physical and Environmental Protection (PE)

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

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 annually]; and
   2. Physical and environmental protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 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 (H)

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 every ninety (90) days]; 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 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 | 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 | GDIT HCSD - Cage 203E –contains the Cage Access History Report |
| Part d | 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 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 | 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 | 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 | The visitor is required to sign-out when leaving the Cloud facility |
| Part d | Biometric finger scanners |
| Part e | COPT conducts a monthly inventory of badge readers and biometric scanners. |
| Part f | 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-3 (1) Control Enhancement (H)

The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing components of the information system].

| PE-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter PE-3 (1): Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### PE-4 Access Control for Transmission Medium (M) (H)

The organization controls physical access to [Assignment: organization-defined information system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security safeguards].

| PE-4 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-4-1: information system distribution and transmission lines | |
| Parameter PE-4-2: 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 | |

| PE-4 What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East: Communication circuits enter the building underground. These transmission lines terminate in one of three access controlled rooms on the bottom floor. Rooms are dedicated to service providers. Conduit is used from the room to upper level suites where GDIT Cloud technology exists. Suite Communication Distribution Boxes created a demarcation point in the suite where connections to customer-specific cages are pulled through trays above. COPT Staff and Security provides reports monthly on controlled systems. |

### PE-5 Access Control for Output Devices (M) (H)

The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

| PE-5 | 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-5 What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East: The data Center is a lights out center with no internal monitors. All GDIT Cloud systems are kept in this closed area with no outside access. The monitors in the Facility NOC are 150 feet from the outside fence. |

### 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 | Cameras and access control systems are monitored 24x7 by the COPT Security Guards. |
| Part b | 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 | 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-6 (1) Control Enhancement (M) (H)

The organization monitors physical intrusion alarms and surveillance equipment.

| PE-6 (1) | 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-6 (1) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East: The Security Guard station and the Facility NOC monitor 24x7 for all alarms (physical intrusion alarms and surveillance equipment). External Door, internal door, hall, and room monitors alert on premise security personnel and staff. Cameras located throughout the facility (internal and external) provide visual awareness of the alarm. |

#### PE-6 (4) Control Enhancement (H)

The organization monitors physical access to the information system in addition to the physical access monitoring of the facility as [Assignment: organization-defined physical spaces containing one or more components of the information system].

| PE-6 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter PE-6 (4): Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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 | 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 | (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-8 (1) Control Enhancement (H)

The organization employs automated mechanisms to facilitate the maintenance and review of visitor access records.

| PE-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### PE-9 Power Equipment and Cabling (M) (H)

The organization protects power equipment and power cabling for the information system from damage and destruction.

| PE-9 | 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-9 What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East: All power systems are secured from clients. Power systems consist of a power feed from multiple transmission sources, a power topology with a backbone designed to accommodate Alternating Current (“AC”) or Direct Current (“DC”) power loads, and a modular design that provides the ability to expand power in place with minimal disruption and lead time. Isolation from the power grid provides Electro Magnetic Pulse (“EMP”) protection and electrical generation that is block redundant, leaving no single point of failure. |

### PE-10 Emergency Shutoff (M) (H)

The organization:

1. Provides the capability of shutting off power to the information system or individual system components in emergency situations;
2. Places emergency shutoff switches or devices in [Assignment: organization-defined location by information system or system component] to facilitate safe and easy access for personnel; and
3. Protects emergency power shutoff capability from unauthorized activation.

| PE-10 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-10(b): ; OC West: emergency power off (EPO) switch located on the outside of the data center door; OC East: There are no emergency power-off buttons in the site. COPT controls the systems in secure areas not accessible by clients | |
| 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-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Security and environmental monitoring systems that are monitored 24x7 from within the onsite Network Operations Center to ensure the security and availability of the facility and campus and that operations meet tenant Service Level Agreement (“SLA”) metrics. If the need arises to shut off power (Computer or UPS rooms, or GDIT Cage) the NOC has the tools (EPO switch) to disable power. Individual system components have built-in power switches and individual busway circuit breakers and switches to kill power in emergency situations. |
| Part b | GDIT Cloud East: Shut-off breakers are located in electrical rooms. |
| Part c | GDIT Cloud East: Shut-off breakers are located in secure rooms. |

### PE-11 Emergency Power (M) (H)

The organization provides a short-term uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the information system; transition of the information system to long-term alternate power] in the event of a primary power source loss.

| PE-11 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-11: transition of the information system to long-term alternate power | |
| 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-11 What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East: UPS systems are provided for information systems. Generators are activated within 7 to 9 seconds. |

#### PE-11 (1) Control Enhancement (H)

The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

| PE-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-11 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| 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? |
| --- |
| 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-13 (1) Control Enhancement (H)

The organization employs fire detection devices/systems for the information system that activate automatically and notify [FedRAMP Assignment: service provider building maintenance/physical security personnel] and [FedRAMP Assignment: service provider emergency responders with incident response responsibilities] in the event of a fire.

| PE-13 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter PE-13 (1)-1: Click or tap here to enter text. | |
| Parameter PE-13 (1)-2: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### PE-13 (2) Control Enhancement (M) (H)

The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders].

| PE-13 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-13(2)-1: building security | |
| Parameter PE-13(2)-2: the local fire department | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East: Dual interlocked Dry pipe with pre-activation requiring two events to occur and a third to activate by zone. All water in maintained below the data center on the bottom level. |

#### PE-13 (3) Control Enhancement (M) (H)

The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

| PE-13 (3) | 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 (3) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud East; The site is staffed 24x7 and capable of responding to alarms. |

### 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: Click or tap here to enter text. | |
| 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 | COPT monitors environmental systems 24x7 from within the onsite Network Operations Center.. |
| Part b | Click or tap here to enter text. |

#### PE-14 (2) Control Enhancement (M) (H)

The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

| PE-14 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Facilities 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 | |

| PE-14 (2) What is the solution and how is it implemented? |
| --- |
| Humidity and Temperature are monitored by COPT. Also, the GDIT Cloud uses Schneider Electric’s APC StruxureWare Data Center Expert to log video, humidity and temperature data from the APC NetBotz environmental monitors deployed inside the GDIT Cloud cage at the East data center. This system shows alerts on the monitors in the NOC and the manager’s office and sends out email alerts when values exceed the threshold. If an email alert is received, the Facilities Manager contacts COPT. COPT on-site personnel determine the cause. If the cause is due to system issues, COPT classifies the event to determine appropriate reponses and personnel to be notified in accordance with the Emergency Escalation Procedure (COPT DC-6 Facilities Manual). |

### 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? |
| --- |
| GDIT Cloud East: Water shut-off valve(s) are located in secure rooms that are one level below. |

#### PE-15 (1) Control Enhancement (H)

The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts [FedRAMP Assignment: service provider building maintenance /physical security personnel].

| PE-15 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter PE-15 (1): Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| 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. |

### PE-17 Alternate Work Site (M) (H)

The organization:

1. Employs [Assignment: organization-defined security controls] at alternate work sites;
2. Assesses as feasible, the effectiveness of security controls at alternate work sites; and
3. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

| PE-17 | Control Summary Information |
| --- | --- |
| Responsible Role: FSO | |
| Parameter PE-17(a): defines management, operational, and technical information system security controls for alternate work sites. The security controls are approved and accepted by the JAB.; ; [\*\*TABLE DROPPED\*\*] | |
| 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-17 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Click or tap here to enter text. |
| Part b | We rely on human responsibility that conforms to the GDIT Cloud Rules of Behavior that commits each GDIT Cloud personnel to use the equipment in a secure and predictable manner. |
| Part c | GDIT Cloud personnel call the Service Desk number (305-542-8498) and to activate a security incident; i.e., loss of laptop, etc. |

### PE-18 Location of Information System Components (H)

The organization positions information system components within the facility to minimize potential damage from [FedRAMP Assignment: physical and environmental hazards identified during threat assessment] and to minimize the opportunity for unauthorized access.

| PE-18 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter PE-18: Click or tap here to enter text. | |
| 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-18 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

## Planning (PL)

### PL-1 Security Planning Policy and Procedures (H)

The organization:

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

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

The organization plans and coordinates security-related activities affecting the information system with [Assignment: organization-defined individuals or groups] before conducting such activities in order to reduce the impact on other organizational entities.

| PL-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PL-2(3): GDIT Cloud ISSO, System Owner, System Manager, and with other relevant teams | |
| 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 (3) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### PL-4 Rules of Behavior (H)

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: annually]; 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 current version of the GDIT ROB is maintained by the ISSO as an appendix to the GDIT Cloud SSP. |
| Part b | 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. |

#### PL-4 (1) Control Enhancement (M) (H)

The organization includes in the rules of behavior, explicit restrictions on the use of social media/ networking sites and posting organizational information on public websites.

| PL-4 (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)  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 (1) What is the solution and how is it implemented? |
| --- |
| In addition, the GDIT Cloud restricts access to social media/networking sites from within the Cloud, and the user agree (through the ROB) dictates that a user is not to bypass the restrictions to access social media/networking sites. |

### PL-8 Information Security Architecture (M) (H)

The organization:

1. Develops an information security architecture for the information system that:
   1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;
   2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and
   3. Describes any information security assumptions about, and dependencies on, external services;
2. Reviews and updates the information security architecture [FedRAMP Assignment: at least annually or when a significant change occurs] to reflect updates in the enterprise architecture; and

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

Guidance: Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F, on Page F-8.

1. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions.

| PL-8 | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter PL-8(b): 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-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Describes any information security assumptions about, and dependencies on, external services |
| Part b | The ISSO reviews and updates the information security architecture at least annually to reflect updates in the enterprise architecture, as directed by the Continuous Monitoring Program. |
| Part c | The ISSO ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions according to the Change Management process. |

## Personnel Security (PS)

### PS-1 Personnel Security Policy and Procedures (H)

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 annually]; and
   2. Personnel security procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 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 (H)

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 annually].

| 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 | Click or tap here to enter text. |
| Part b | 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 | Click or tap here to enter text. |
| Part b | At a minimum, all staff go through a five-year public trust reinvestigation. |

#### PS-3 (3) Control Enhancement (M) (H)

The organization ensures that individuals accessing an information system processing, storing, or transmitting information requiring special protection:

1. Have valid access authorizations that are demonstrated by assigned official government duties; and
2. Satisfy [FedRAMP Assignment: personnel screening criteria – as required by specific information].

| PS-3 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Account Managers | |
| Parameter PS-3 (3)(b): personnel screening criteria – as required by specific information | |
| 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 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | and documented in the request for access ticket. |
| Part b | HR obtains the prerequisite security authorizations prior to on-boarding the individual |

### PS-4 Personnel Termination (H)

The organization, upon termination of individual employment:

1. Disables information system access within [FedRAMP Assignment: eight (8) hours];
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: 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 | 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-4 (2) Control Enhancement (H)

The organization employs automated mechanisms to notify [FedRAMP Assignment: access control personnel responsible for disabling access to the system] upon termination of an individual.

| PS-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter PS-4 (2): Click or tap here to enter text. | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### PS-5 Personnel Transfer (H)

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 [FedRAMP Assignment: twenty-four (24) hours];
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: twenty-four (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 | 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 | 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 (H)

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 and any time there is a change to the user's level of access].

| 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 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 (H)

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: terminations: immediately; transfers: within twenty-four (24) hours]; 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 | 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 (H)

The organization:

1. Employs a formal sanctions process for personnel failing to comply with established information security policies and procedures; and
2. Notifies [FedRAMP Assignment: at a minimum, the ISSO and/or similar role within the organization] 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 (H)

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 annually]; and
   2. Risk assessment procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 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 | 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 | 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 (H)

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 | 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 | 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 | 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 | 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 | The GDIT Cloud ISSO reviews the POA&M list to ensure that it is in compliance with the FedRAMP standards. |
| Part e | Acunetix, as documented in KA 11286, How To: FedRAMP - Web Application scanning : FedRAMP ISSO, OMNI Director of Engineering, ConMon Project Manager. |

#### RA-5 (1) Control Enhancement (M) (H)

The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities to be scanned.

| RA-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Security 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 | |

| RA-5 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### RA-5 (2) Control Enhancement (M) (H)

The organization updates the information system vulnerabilities scanned [Selection (one or more): [FedRAMP Assignment: prior to a new scan]].

| RA-5 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| Parameter RA-5(2): prior to a new scan | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| These updates are documented in tickets and accomplished in accordance with the Security Calendar. More regular updates are accomplished as desired. |

#### RA-5 (3) Control Enhancement (M) (H)

The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

| RA-5 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| 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 (3) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud MMS Vulnerability Tools scans all servers and networking operating system deployed within the GDIT Cloud security authorization boundary. GDIT Cloud MMS Vulnerability Tools are used to scan the MSSql databases. GDIT Cloud MMS Vulnerability Tools is used to scan all web applications within the GDIT Cloud security authorization boundary. All scans performed are credentialed, when supported by the vendors. |

#### RA-5 (4) Control Enhancement (H)

The organization determines what information about the information system is discoverable by adversaries and subsequently takes [FedRAMP Assignment: notify appropriate service provider personnel and follow procedures for organization and service provider-defined corrective actions].

| RA-5 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter RA-5 (4): Click or tap here to enter text. | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### RA-5 (5) Control Enhancement (M) (H)

The organization includes privileged access authorization to [FedRAMP Assignment: operating systems, databases, web applications] for selected [FedRAMP Assignment: all scans].

| RA-5 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| Parameter RA-5(5)-1: operating systems, databases, web applications | |
| Parameter RA-5(5)-2: all scans | |
| 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 (5) What is the solution and how is it implemented? |
| --- |
| The account managers use the standard AD account creation process for scan tool privileged access. |

#### RA-5 (6) Control Enhancement (M) (H)

The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

| RA-5 (6) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| 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 (6) What is the solution and how is it implemented? |
| --- |
| The tools used for scanning are automated and provide the capability of comparing historical vulnerability scan results for the purposes of trend analysis. Additionally, these tools automatically captures scan results for review and then captures the resulting actions in the ticket system, tracks the review, documents the resolution if any needed, and retains the ticket for comparison to future scans. The results from other tools are captured into the ticketing system directly. |

#### RA-5 (8) Control Enhancement (L) (M) (H)

The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

RA-5(8) Additional FedRAMP Requirements and Guidance:

Requirement: This enhancement is required for all high vulnerability scan findings.

Guidance: While scanning tools may label findings as high or critical, the intent of the control is based around NIST's definition of high vulnerability.

| RA-5 (8) | 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-5 (8) What is the solution and how is it implemented? |
| --- |
| In the event of an identified compromise, SOC analysts produce the raw log information to identify patterns of compromise behavior. Then Security Engineers write new correlation rules based on those behavior patterns and apply them to previously recorded logs for further identification of compromised systems. |

#### RA-5 (10) Control Enhancement (H)

The organization correlates the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.

RA-5 (10) Additional FedRAMP Requirements and Guidance:

Guidance: If multiple tools are not used, this control is not applicable.

| RA-5 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (10) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

## System and Services Acquisition (SA)

### SA-1 System and Services Acquisition Policy and Procedures (H)

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 annually]; and
   2. System and services acquisition procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 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 | 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 | 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 | 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 | Click or tap here to enter text. |
| Part d | 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 | Click or tap here to enter text. |
| 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 | 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 | Click or tap here to enter text. |
| 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-4 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.

| SA-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System 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 | |

| SA-4 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SA-4 (2) Control Enhancement (H)

The organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [FedRAMP Selection (one or more): at a minimum to include security-relevant external system interfaces; high-level design; low-level design; source code or network and data flow diagram; [organization-defined design/implementation information]]at [Assignment: organization-defined level of detail].

| SA-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| Parameter SA-4-1: to include security-relevant external system interfaces and high-level design | |
| Parameter SA-4-2: organization-defined design/implementation information | |
| Parameter SA-4-3: organization-defined level of detail | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud is also required to follow HCSD-SEC-POL-05, Vendor Security Impact Management, which describes guidance on managing security impacts for GDIT HCSD third party vendors and application service providers (ASPs) that provide personnel, custom products, or services that directly support the delivery of GDIT HCSD information management services. |

#### SA-4 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to produce a plan for the continuous monitoring of security control effectiveness that contains [FedRAMP Assignment: at least the minimum requirement as defined in control CA-7].

SA-4 (8) Additional FedRAMP Requirements and Guidance:

Guidance: CSP must use the same security standards regardless of where the system component or information system service is acquired.

| SA-4 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SA-4(8): Click or tap here to enter text. | |
| 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 (8) What is the solution and how is it implemented? |
| --- |
| At this time, the GDIT Cloud does not acquire services from external sources and therefore the development of additional continuous monitoring plans outside the scope identified under control CA-7 is not necessary. Components to be integrated into the GDIT Cloud are evaluated but the ISSO or SOC manager, for capability consistent with existing continuous monitoring requirements of CA-7, prior to acquisition, during the Security Impact Assessment portion of the System Development Lifecycle (SDLC) identified in control SA-3, part a. Consistency with, and supportability of the continuous monitoring plan is required for acquisition approval. |

#### SA-4 (9) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.

| SA-4 (9) | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| 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 (9) What is the solution and how is it implemented? |
| --- |
| The System Manager requires that service providers identify early in the system development life cycle, the functions, ports, protocols, and services (FPPS) intended for organizational use.The CAB review process takes into account the technical design and security impact before authorizing a change to the system. Information from the service provider regarding FPPS is included in system design documentation and is updated as required in the traffic flow policy (SC-7(4)) and enforced through the implementation of CM-7b and AC-4. |

#### SA-4 (10) Control Enhancement (M) (H)

The organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

| SA-4 (10) | 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 | |

| SA-4 (10) What is the solution and how is it implemented? |
| --- |
| Four (4) virtual appliances encompass the CA-PAM architecture that is clustered for High Availability and Redundancy: two (2) PAM appliances in WCO and two (2) PAM appliances in MVA. |

### SA-5 Information System Documentation (H)

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 [FedRAMP Assignment: at a minimum, the ISSO (or similar role within the organization)].

| 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 | 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 | 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-8 Security Engineering Principles (M) (H)

The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

| SA-8 | 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-8 What is the solution and how is it implemented? |
| --- |
| Implement System Security Assess Information Protection Effectiveness |

### 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. |

#### SA-9 (1) Control Enhancement (M) (H)

The organization:

1. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and
2. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].

| SA-9 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SA-9(1)(b): Approved 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 | |

| SA-9 (1) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | For any type of changes to the infrastructure or for acquisition or outsourcing of security services, the ISSO provides a security impact analysis as part of the CAB review and approval process to assess the risk. |
| Part b | If externally dedicated information security services are ever considered, GDIT Cloud System Manager will request approval from the Joint Authorization Board (JAB). |

#### SA-9 (2) Control Enhancement (M) (H)

The organization requires providers of [FedRAMP Assignment: All external systems where Federal information is processed or stored] to identify the functions, ports, protocols, and other services required for the use of such services.

| SA-9 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SA-9(2): All 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 (2) What is the solution and how is it implemented? |
| --- |
| Per GDIT Cloud Security Policy, the GDIT Cloud does not process or store federal information on external systems. |

#### SA-9 (4) Control Enhancement (M) (H)

The organization employs [Assignment: organization-defined security safeguards] to ensure that the interests of [FedRAMP Assignment: All external systems where Federal information is processed or stored] are consistent with and reflect organizational interests.

| SA-9 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: System Manager | |
| Parameter SA-9(4)-1: Meet moderate requirements of NIST, as specific; FIPS 140-2 for transmission; multi-factor authentication; Hardening guidelines; FedRAMP Technical controls; FedRAMP Operational controls; Be subject to monitoring | |
| Parameter SA-9(4)-2: All external systems where Federal information is processed or store | |
| 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 (4) What is the solution and how is it implemented? |
| --- |
| Be subject to monitoring |

#### SA-9 (5) Control Enhancement (M) (H)

The organization restricts the location of [FedRAMP Selection: information processing, information data, AND information services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].

Additional FedRAMP Requirements and Guidance

Guidance: System services refer to FTP, Telnet, and TFTP, etc.

| SA-9 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SA-9(5)-1: information processing, information data AND information services | |
| Parameter SA-9(5)-2: GDIT Cloud locations | |
| Parameter SA-9(5)-3: FedRAMP security requirements | |
| 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 (5) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud does not use external information system services for processing data; therefore, this control is N/A at this time. |

### SA-10 Developer Configuration Management (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Perform configuration management during system, component, or service [FedRAMP Selection: development, implementation, AND operation];
2. Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
3. Implement only organization-approved changes to the system, component, or service;
4. Document approved changes to the system, component, or service and the potential security impacts of such changes; and
5. Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].

SA-10 (e) Additional FedRAMP Requirements and Guidance:

Requirement: For JAB authorizations, track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel, to include FedRAMP.

| SA-10 | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| Parameter SA-10(a): development, implementation, AND operation | |
| Parameter SA-10(b): configuration items under configuration management | |
| Parameter SA-10(e): The System Developer performs configuration management during system, component, or service development, implementation, and operation according the GDIT Cloud Service Asset and Configuration Management Process and Procedures 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-10 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The System Developer documents, manages, and controls the integrity of changes to configuration items under configuration management according the GDIT Cloud Service Asset and Configuration Management Process and Procedures Guide. |
| Part b | The System Developer implements only organization-approved changes to the system according to the GDIT Cloud Change Management Process and Procedures Guide. |
| Part c | The System Developer documents approved changes to the system, component, or service and the potential security impacts of such changes as part of the approved CR ticket as part of the GDIT Cloud Change Management Process and Procedures Guide. |
| Part d | The System Developer tracks security flaws and flaw resolution within the system, component, or service and report findings to the CAB as part of the GDIT Cloud Change Management Process and Procedures Guide. |
| Part e | Click or tap here to enter text. |

#### SA-10 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to enable integrity verification of software and firmware components.

| SA-10 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| 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-10 (1) What is the solution and how is it implemented? |
| --- |
| GDIT uses only COTS software and does not do any software development for the Cloud development. Currently, Therefore, this control is NA, since this function is performed by the product vendor. |

### SA-11 Developer Security Testing and Evaluation (M) (H)

The organization requires the developer of the information system, system component, or information system service to:

1. Create and implement a security assessment plan;
2. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage];
3. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;
4. Implement a verifiable flaw remediation process; and
5. Correct flaws identified during security testing/evaluation.

| SA-11 | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| Parameter SA-11(b)-1: unit; integration; system; regression | |
| Parameter SA-11(b)-2: ; Voice-perspective Testing; Test whether toll-free number identifies proper target.; Test whether routing plans followed create path through section.; Test whether sessions do not co-mingle; Chat-perspective Testing; Test whether website itself has proper key value pairs within the session that ID for each customer for proper routing.; Test the skills and key value pairs routing strategy and that it is routed to appropriate place.; Network Testing; Test that ports communicating link is working properly; Test that firewall rules are defined properly | |
| 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-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Part of the change management process includes a security assessment plan that is an input to the CAB review and documented in the RFC ticket and stored in Cherwell. |
| Part b | Once the test plan (security assessment plan) is approved by the CAB, the integration team performs unit testing, system testing, integration testing, and customer acceptance testing during the testing phase, integration phase, and deployment phase of the SDLC. |
| Part c | The implementation team produces evidence of the execution of the security assessment plan and the results of the security testing/evaluation through the test plan results which are documented in the RFC and stored in Cherwell. |
| Part d | After deployment, flaws are identified as CRs that are tracked to completion in the Cherwell ticket system and are closed according to the Change Management process. |
| Part e | After deployment, flaws are remediated as part of the RFC, which also includes a Deployment & Backout plan that includes all of the steps for the deployment including the exit/result criteria. |

#### SA-11 (1) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ static code analysis tools to identify common flaws and document the results of the analysis.

SA-11 (1) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider documents in the Continuous Monitoring Plan, how newly developed code for the information system is reviewed.

| SA-11 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| 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-11 (1) What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud uses only COTS products. There is no development activity that changes the base product code. All changes to the GDIT Cloud are configuration changes. Consequently, GDIT relies on the COTS product vendor developers to employ static code analysis tools to identify common flaws and document the results of the analysis within their process. |

#### SA-11 (2) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/ evaluation of the as-built system, component, or service.

| SA-11 (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-11 (2) What is the solution and how is it implemented? |
| --- |
| Post-implementation vulnerability analysis is performed through ad-hoc and monthly Nessus scans by GDIT Cloud security personnel. Scans are run via Tenable Security Center (Nessus) by the vulnerability management team as soon as the implementation is completed. Engineers open a Cherwell incident ticket for the scan to be completed when implementation is complete. The Vulnerability Manager provides the vulnerability report to the Engineer as soon as the scan is complete. This allows for quick remediation of any unexpected findings. Further details on vulnerability scanning can be found in the section for RA-5. |

#### SA-11 (8) Control Enhancement (M) (H)

The organization requires the developer of the information system, system component, or information system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.

| SA-11 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: System Developer | |
| 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-11 (8) What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud uses COTS products. There is no development activity that changes the base product code. All changes to the GDIT Cloud are configuration changes. Consequently, GDIT relies on the COTS product vendor developers to employ dynamic code analysis tools to identify common flaws and document the results of the analysis within their process. |

### SA-12 Supply Chain Protection (H)

The organization protects against supply chain threats to the information system, system component, or information system service by employing [FedRAMP Assignment: organization and service provider-defined personnel security requirements, approved HW/SW vendor list/ process, and secure SDLC procedures] as part of a comprehensive, defense-in-breadth information security strategy.

| SA-12 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SA-12: Click or tap here to enter text. | |
| 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-12 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SA-15 Development Process, Standards, and Tools (H)

The organization:

1. Requires the developer of the information system, system component, or information system service to follow a documented development process that:
   1. Explicitly addresses security requirements;
   2. Identifies the standards and tools used in the development process;
   3. Documents the specific tool options and tool configurations used in the development process; and
   4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and
2. Reviews the development process, standards, tools, and tool options/configurations [FedRAMP Assignment: as needed and as dictated by the current threat posture] to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy [FedRAMP Assignment: organization and service provider- defined security requirements].

| SA-15 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SA-15 (b)-1: Click or tap here to enter text. | |
| Parameter SA-15 (b)-2: Click or tap here to enter text. | |
| 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-15 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. |

### SA-16 Developer-Provided Training (H)

The organization requires the developer of the information system, system component, or information system service to provide [Assignment: organization-defined training] on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

| SA-16 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SA-16: Click or tap here to enter text. | |
| 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-16 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SA-17 Developer Security Architecture and Design (H)

The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that:

1. Is consistent with and supportive of the organization’s security architecture which is established within and is an integrated part of the organization’s enterprise architecture;
2. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and
3. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

| SA-17 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-17 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. |
| Part c | Click or tap here to enter text. |

## System and Communications Protection (SC)

### SC-1 System and Communications Protection Policy and Procedures (H)

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 annually]; and
   2. System and communications protection procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 Knowledge Manager changes the KA’s review date to the following year. (If the update was done based on the annual review.) |

### SC-2 Application Partitioning (M) (H)

The information system separates user functionality (including user interface services) from information system management functionality.

| SC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers and 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 | |

| SC-2 What is the solution and how is it implemented? |
| --- |
| Management is logically separated into VLANS that are protected by an internal firewall which provides ports and protocols for access. |

### SC-3 Security Function Isolation (H)

The information system isolates security functions from non-security functions.

| SC-3 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-3 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SC-4 Information in Shared Resources (M) (H)

The information system prevents unauthorized and unintended information transfer via shared system resources.

| SC-4 | 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 | |

| SC-4 What is the solution and how is it implemented? |
| --- |
| The use of Adapter-FEX coupled with VM-FEX on the VMs extends the network fabric down to the Hypervisor of the ESXi host. VMware Virtual Machines (VMs) utilize the Cisco Nexus 1000v software switch, which enables the VMs to support the requirements of the Cloud; such as, policy-based networking, mobile VM security, and VM aware event. This takes the virtual switching burden from the software Hypervisor and places it on the fabric extenders to increase response and availability.  The 1000V provides the extension of the Access Layer connection at the Fabric Interconnects down into the VM software. The 1000V also provides the integration with vCenter and allows monitoring of the vNIC and management capabilities.  This creates the required port channels and defines QoS, security, and monitoring down to into the vNIC. |

### 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? |
| --- |
| 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-6 Resource Availability (M) (H)

The information system protects the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined security safeguards]].

| SC-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-6-1: Server capacity | |
| Parameter SC-6-2: Quota | |
| Parameter SC-6-3: priority status implementation | |
| 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-6 What is the solution and how is it implemented? |
| --- |
| At this time, there are sufficient resources in the GDIT Cloud to operate at full capacity. At such time when resources are constricted due to a growth in our architecture, we will implement applications with priority status to insure that key applications (security applications) will always obtain required resources to operate efficiently and effectively in monitoring the Cloud. |

### 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 | 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 | 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 | 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-7 (3) Control Enhancement (M) (H)

The organization limits the number external network connections to the information system.

| SC-7 (3) | 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-7 (3) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SC-7 (4) Control Enhancement (H)

The organization:

1. Implements a managed interface for each external telecommunication service;
2. Establishes a traffic flow policy for each managed interface;
3. Protects the confidentiality and integrity of the information being transmitted across each interface;
4. Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and
5. Reviews exceptions to the traffic flow policy [FedRAMP Assignment: at least every ninety (90) days or whenever there is a change in the threat environment that warrants a review of the exceptions] and removes exceptions that are no longer supported by an explicit mission/business need.

| SC-7 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-7(4)(e): 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 | |

| SC-7 (4) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Click or tap here to enter text. |
| Part b | The GDIT Cloud establishes a traffic flow policy for each managed interface through the customer routing and firewall rules that are defined in the customer requirements to expose the ports that the components use to communicate to deliver the service necessary for each specific customer channel. |
| Part c | The GDIT Cloud protects the confidentiality and integrity of the information being transmitted across each interface through workflow rules and port assignments that enforce customer data segregation. |
| Part d | The GDIT Cloud documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need. However, since the traffic flow policy determines mandated customer separation, there is no exception to the traffic flow policy. |
| Part e | The GDIT Cloud ISSO reviews exceptions to the traffic flow policy at least annually and removes exceptions that are no longer supported by an explicit mission/business need as part of continuous monitoring. |

#### SC-7 (5) Control Enhancement (M) (H)

The information system at managed interfaces denies network traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception).

| SC-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Network 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 | |

| SC-7 (5) What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud Border Guard firewalls are the managed interfaces of the GDIT Cloud. The firewalls are configured with traffic flow policies as represented by the ports, protocols, and services in SC 7-4 (d). With the exception of these services, the firewall is configured in a “Deny IP any any log” method of operation. |

#### SC-7 (7) Control Enhancement (M) (H)

The information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.

| SC-7 (7) | 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-7 (7) What is the solution and how is it implemented? |
| --- |
| Split tunneling is not permitted for remote connections into the GDIT Cloud. Bridging by a remote external device is restricted by the acceptable use policy and rules of behavior. All network connections are managed by the GDIT Cloud Border Guard. See SC-7 for more information. |

#### SC-7 (8) Control Enhancement (M) (H)

The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.

| SC-7 (8) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-7(8)-1: program-specific internal communications traffic | |
| Parameter SC-7(8)-2: GDIT external networks | |
| 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 (8) What is the solution and how is it implemented? |
| --- |
| Currently, Firepower manages multiple groups. One group supports the GDIT Cloud workstations. Another group supports Customers, who must request Internet access and get approval from the GDIT Cloud CAB.  At this time there are three requests: Virtual Desktop Infrastructure (VDI), Homeland Security Information Network (HSIN), and EFAX.  These groups have policies applied to them and are managed in a “white list” approach, as opposed to generically approved categories.  New entries to the initial, approved “white lists” require Security and Operations approval, pending proper business justification followed by CAB approval. |

#### SC-7 (10) Control Enhancement (H)

The organization prevents the unauthorized exfiltration of information across managed interfaces.

| SC-7 (10) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (10) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SC-7 (12) Control Enhancement (H)

The organization implements [FedRAMP Assignment: Host Intrusion Prevention System (HIPS), Host Intrusion Detection System (HIDS), or minimally a host-based firewall] at [Assignment: organization-defined information system components].

| SC-7 (12) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SC-7(12)-1: VLAN segmentation | |
| Parameter SC-7(12)-2: GDIT Cloud 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 | |

| SC-7 (12) What is the solution and how is it implemented? |
| --- |
| Linux machines have IPTables installed and configured and use OSSEC for file-based monitoring. In addition, Symantec AntiVirus (SAV) is installed for antivirus. |

#### SC-7 (13) Control Enhancement (H)

The organization isolates [FedRAMP Assignment: See SC-7 (13) additional FedRAMP Requirements and Guidance] from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

SC-7 (13) Additional FedRAMP Requirements and Guidance:

Requirement: The service provider defines key information security tools, mechanisms, and support components associated with system and security administration and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets.

Guidance: Examples include: information security tools, mechanisms, and support components such as, but not limited to public key infrastructure (PKI), patching infrastructure, cyber defense tools, special purpose gateway, vulnerability tracking systems, internet access points (IAPs); network element and data center administrative/management traffic; demilitarized zones (DMZs), Server farms/computing centers, centralized audit log servers, etc.

| SC-7 (13) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter SC-7(13): key information security tools, mechanisms, and support components associated with system and security administration and isolates those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnets. | |
| 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 (13) What is the solution and how is it implemented? |
| --- |
| The internal firewall manages the interface to VLAN, thus providing separation against attacks. |

#### SC-7 (18) Control Enhancement (M) (H)

The information system fails securely in the event of an operational failure of a boundary protection device.

| SC-7 (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 | |

| SC-7 (18) What is the solution and how is it implemented? |
| --- |
| In the event of a firewall system failure, the GDIT Cloud will fail securely, in that public-facing interfaces are shut down. A failure of a Border Guard protection firewall cannot lead to or cause information external to the system to enter the device, nor can a failure permit unauthorized information release. |

#### SC-7 (20) Control Enhancement (H)

The information system provides the capability to dynamically isolate/segregate [Assignment: organization-defined information system components] from other components of the system.

| SC-7 (20) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SC-7 (20): Click or tap here to enter text. | |
| 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 (20) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SC-7 (21) Control Enhancement (H)

The organization employs boundary protection mechanisms to separate [Assignment: organization-defined information system components] supporting [Assignment: organization-defined mission and/or business functions].

| SC-7 (21) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SC-7 (21)-1: Click or tap here to enter text. | |
| Parameter SC-7 (21)-2: Click or tap here to enter text. | |
| 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 (21) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SC-8 Transmission confidentiality and Integrity (M) (H)

The information system protects the [FedRAMP Assignment: confidentiality AND integrity] of transmitted information.

| SC-8 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-8: confidentiality AND integrity | |
| 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-8 What is the solution and how is it implemented? |
| --- |
| 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. |

#### SC-8 (1) Control Enhancement (M) (H)

The information system implements cryptographic mechanisms to [FedRAMP Assignment: prevent unauthorized disclosure of information AND detect changes to information] during transmission unless otherwise protected by [FedRAMP Assignment: a hardened or alarmed carrier Protective Distribution System (PDS)].

| SC-8 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SC-8 (1)-1: prevent unauthorized disclosure of information AND detect changes to information | |
| Parameter SC-8 (1)-2: a hardened or alarmed carrier Protective Distribution System (PDS) | |
| 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-8 (1) What is the solution and how is it implemented? |
| --- |
| Other communications that cross the FedRAMP boundary use HTTPS sessions with FIPS 140-2 compliant cryptographic modules with FIPS approved ciphers. |

### SC-10 Network Disconnect (H)

The information system terminates the network connection associated with a communications session at the end of the session or after [FedRAMP Assignment: no longer than ten (10) minutes for privileged sessions and no longer than fifteen (15) minutes for user sessions] of inactivity.

| SC-10 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter SC-10: thirty minutes for all RAS-based sessions; thirty to sixty minutes for non-interactive users and long running batch jobs and other operations are not subject to this time limit. | |
| 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-10 What is the solution and how is it implemented? |
| --- |
| Table 11-11. User Access Timeout / Re-Authentication |

### 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? |
| --- |
| 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-12 (1) Control Enhancement (H)

The organization maintains availability of information in the event of the loss of cryptographic keys by users.

| SC-12 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SC-12 (2) Control Enhancement (M) (H)

The organization produces, controls, and distributes symmetric cryptographic keys using [FedRAMP Selection: NIST FIPS-compliant] key management technology and processes.

| SC-12 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter SC-12 (2): NIST FIPS-compliant | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SC-12 (3) Control Enhancement (M) (H)

The organization produces, controls, and distributes asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].

| SC-12 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineer | |
| Parameter SC-12 (3): NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key | |
| 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 (3) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| 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 (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: 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-17 Public Key Infrastructure Certificates (M) (H)

The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider.

| SC-17 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter SC-17: organization-defined certificate policy | |
| 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-17 What is the solution and how is it implemented? |
| --- |
| 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. |

### SC-18 Mobile Code (M) (H)

The organization:

1. Defines acceptable and unacceptable mobile code and mobile code technologies;
2. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and
3. Authorizes, monitors, and controls the use of mobile code within the information system.

| SC-18 | 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-18 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | The GDIT Cloud does not utilize mobile code.  The website is publically accessible, meaning it can be accessed via mobile device with a compatible browser, but the same security measures, including multifactor authentication, apply. |
| Part b | Based on the GDIT Cloud Security Policy, there are no mobile code technologies within IaaS, but if introduced, they would require approval by the CAB. Currently, only COTS approved products are used. |
| Part c | Mobile code technologies are authorized by the CAB and/or JAB. White listing technology within the GDIT Cloud MMS provides monitoring of all Web servers that access the internet and workstations. |

### SC-19 Voice Over Internet Protocol (M) (H)

The organization:

1. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and
2. Authorizes, monitors, and controls the use of VoIP within the information system.

| SC-19 | Control Summary Information |
| --- | --- |
| Responsible Role: Network 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 | |

| SC-19 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | If VOIP is used in a customer environment, the Customer is responsible for establishing usage restrictions and implementation guidance for VOIP technologies based on the potential to cause damage to the information system if used maliciously. |
| Part b | If VOIP is used in a Customer environment, the Customer is responsible for authorizing, monitoring, and controlling the use of VOIP within the information system. |

### 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 | 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 | 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? |
| --- |
| Click or tap here to enter text. |

### 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? |
| --- |
| Provide name/address resolution service for an organization and are fault-tolerant and implement internal/external role separation. |

### SC-23 Session Authenticity (M) (H)

The information system protects the authenticity of communications sessions.

| SC-23 | Control Summary Information |
| --- | --- |
| Responsible Role: Network 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 | |

| SC-23 What is the solution and how is it implemented? |
| --- |
| 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. |

#### SC-23 (1) Enhancement (H)

The information system invalidates session identifiers upon user logout or other session termination.

| SC-23 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-23 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SC-24 Fail in Known State (H)

The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure.

| SC-24 | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SC-24-1: Click or tap here to enter text. | |
| Parameter SC-24-2: Click or tap here to enter text. | |
| Parameter SC-24-3: Click or tap here to enter text. | |
| 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-24 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SC-28 Protection of Information at Rest (M) (H)

The information system protects the [FedRAMP Selection: confidentiality AND integrity]] of [Assignment: organization-defined information at rest].

SC-28 Additional FedRAMP Requirements and Guidance:

Guidance: The organization supports the capability to use cryptographic mechanisms to protect information at rest.

| SC-28 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter SC-28-1: confidentiality AND integrity | |
| Parameter SC-28-2: configuration data | |
| 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-28 What is the solution and how is it implemented? |
| --- |
| The Customer is responsible for the encryption of sensitive data at rest within the Virtual Machine’s operating system and applications. Encryption services are a custom feature that must be requested by the Customer. |

#### SC-28 (1) Control Enhancement (H)

The information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined information] on [FedRAMP Assignment: all information system components storing customer data deemed sensitive]

| SC-28 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SC-28(1)-1: Vulnerability Scan data | |
| Parameter SC-28(1)-2: Tenable SecurityCenter | |
| 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-28 (1) What is the solution and how is it implemented? |
| --- |
| In addition, the Security Engineers encrypt SecurityCenter through SafeNet, as well as protect the key store with SafeNet Key Manager through the HSM key management appliance, which is FIPS-140-2 certified by NIST. |

### 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? |
| --- |
| 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 (H)

The organization:

1. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
2. A system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
3. Procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls; and
4. Reviews and updates the current:
5. System and information integrity policy [FedRAMP Assignment: at least annually]; and
6. System and information integrity procedures [FedRAMP Assignment: at least annually or whenever a significant change occurs].

| 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 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 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 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 | 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 | 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 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-2 (1) Control Enhancement (H)

The organization centrally manages the flaw remediation process.

| SI-2 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-2 (2) Control Enhancement (M) (H)

The organization employs automated mechanisms [FedRAMP Assignment: at least monthly] to determine the state of information system components with regard to flaw remediation.

| SI-2 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SI-2 (2): 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 | |

| SI-2 (2) What is the solution and how is it implemented? |
| --- |
| Subsequent results of the scans are compared to help ensure that remediation efforts for identified vulnerabilities are effective. |

#### SI-2 (3) Control Enhancement (M) (H)

The organization:

1. Measures the time between flaw identification and flaw remediation; and
2. Establishes [Assignment: organization-defined benchmarks] for taking corrective actions.

| SI-2 (3) | Control Summary Information |
| --- | --- |
| Responsible Role: ISSO | |
| Parameter SI-2(3)(b): 72 hours | |
| 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 (3) What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Compliance measurement tools produce weekly reports. As flaws are identified, a ticket is created by the Vulnerability Manager in Cherwell and assigned to the appropriate department for remediation. The Change Manager generates a monthly report from Cherwell that measures the ticket lifespan, briefed to the management team. |
| Part b | The GDIT Cloud ISSO establishes the benchmark for flaw remediation related to configuration compliance or the continuous monitoring vulnerability scan relative to baseline is 72 hours from detection to correction. If the remediation is to exceed that timespan, the ISSO establishes monthly POA&M schedules and metrics for taking corrective actions. |

### SI-3 Malicious Code Protection (H)

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 blocking and quarantining malicious code and alerting administrator or defined security personnel near-real-time] 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 | 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 | 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 | 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 | Because the analysis of all alerts incorporates False Positive determination before responsive action is taken, there is no negative impact to system availability. |

#### SI-3 (1) Control Enhancement (M) (H)

The organization centrally manages malicious code protection mechanisms.

| SI-3 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud MMS host-based protection agents are centrally managed by Security Analysts and BOC |

#### SI-3 (2) Control Enhancement (M) (H)

The information system automatically updates malicious code protection mechanisms.

| SI-3 (2) | 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 | |

| SI-3 (2) What is the solution and how is it implemented? |
| --- |
| These changes are performed per our configuration management policy and procedures. |

#### SI-3 (7) Control Enhancement (M) (H)

The information system implements nonsignature-based malicious code detection mechanisms.

| SI-3 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Network 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 | |

| SI-3 (7) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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 | 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 | 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 | 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 | 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 | \*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 | 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-4 (1) Control Enhancement (M) (H)

The organization connects and configures individual intrusion detection tools into an information system-wide intrusion detection system.

| SI-4 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Security 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 | |

| SI-4 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-4 (2) Control Enhancement (M) (H)

The organization employs automated tools to support near real-time analysis of events.

| SI-4 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analyst | |
| 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 (2) What is the solution and how is it implemented? |
| --- |
| The GDIT Cloud MMS SIEM has intelligence built in using correlation rules that look for specific strings or combinations of strings in all logging data documented in SI-4(1). Based on these correlation rules, the severity of events can be increased or decreased as appropriate. The SIEM performs this operation as the logs are communicated to the SIEM. When correlation rules identify anomalous activity as further described in SI-4(4) below, it issues an Event in Cherwell which is reviewed by the SOC analyst on duty. |

#### SI-4 (4) Control Enhancement (M) (H)

The information system monitors inbound and outbound communications traffic [FedRAMP Assignment: continuously] for unusual or unauthorized activities or conditions.

| SI-4 (4) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Analysts | |
| Parameter SI-4(4): 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 | |

| SI-4 (4) What is the solution and how is it implemented? |
| --- |
| Based on threat information, Firepowers and host-based information systems are updated with current threat information by the vendor. |

#### SI-4 (5) Control Enhancement (M) (H)

The information system alerts [Assignment: organization-defined personnel or roles] when the following indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

SI-4 (5) Additional FedRAMP Requirements and Guidance:

Guidance: In accordance with the incident response plan.

| SI-4 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SI-4(5)-1: 1: ISSO, System Manager, Security Analysts | |
| Parameter SI-4(5)-2: protected information system files or directories have been modified without notification from the appropriate change/configuration management channels; information system performance indicates resource consumption that is inconsistent with expected operating conditions; auditing functionality has been disabled or modified to reduce audit visibility; audit or log records have been deleted or modified without explanation; information system is raising alerts or faults in a manner that indicates the presence of an abnormal condition; resource or service requests are initiated from clients that are outside of the expected client membership set; information system reports failed logins or password changes for administrative or key service accounts; processes and services are running that are outside of the baseline system profile; utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose | |
| 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 (5) What is the solution and how is it implemented? |
| --- |
| Based on the information generated by the IDS system and the HIDS/Integrity configuration and the way that data is fed into the GDIT Cloud Network Monitoring and Alerting system any alerts are generated and received in near real time for the IDS and Daily for GDIT Cloud MMS. |

#### SI-4 (11) Control Enhancement (H)

The organization analyzes outbound communications traffic at the external boundary of the information system and selected [Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)] to discover anomalies.

| SI-4 (11) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SI-4 (11): Click or tap here to enter text. | |
| 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 (11) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-4 (14) Control Enhancement (M) (H)

The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

| SI-4 (14) | Control Summary Information |
| --- | --- |
| Responsible Role: SOC 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 | |

| SI-4 (14) What is the solution and how is it implemented? |
| --- |
| The SOP contains an attached document (GDIT Cloud Wireless Access Point Access Point.docx) that is used to track wireless networks in close proximity to the GDIT Cloud data center. (Example below.) |

#### SI-4 (16) Control Enhancement (M) (H)

The organization correlates information from monitoring tools employed throughout the information system.

| SI-4 (16) | Control Summary Information |
| --- | --- |
| Responsible Role: Security 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 | |

| SI-4 (16) What is the solution and how is it implemented? |
| --- |
| Audit data is never removed from the server; rather it is copied by an OSSEC HID to the GDIT Cloud SIEM where the data is modified (normalized) so correlation and alerting rules in the AlienVault USM server can trigger an event if the alert condition is realized. The AlienVault Logger stores all the event logs in a SQL data base. |

#### SI-4 (18) Control Enhancement (H)

The organization analyzes outbound communications traffic at the external boundary of the information system (i.e., system perimeter) and at [Assignment: organization-defined interior points within the system (e.g., subnetworks, subsystems)] to detect covert exfiltration of information.

| SI-4 (18) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SI-4 (18): Click or tap here to enter text. | |
| 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 (18) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-4 (19) Control Enhancement (H)

The organization implements [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.

| SI-4 (19) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SI-4 (19)-1: Click or tap here to enter text. | |
| Parameter SI-4 (19)-2: Click or tap here to enter text. | |
| 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 (19) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-4 (20) Control Enhancement (H)

The organization implements [Assignment: organization-defined additional monitoring] of privileged users.

| SI-4 (20) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (20) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-4 (22) Control Enhancement (H)

The information system detects network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes] and [Selection (one or more): audits; alerts [Assignment: organization-defined personnel or roles]].

| SI-4 (22) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SI-4 (22)-1: Click or tap here to enter text. | |
| Parameter SI-4 (22)-2: Click or tap here to enter text. | |
| 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 (22) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-4 (23) Control Enhancement (M) (H)

The organization implements [Assignment: organization-defined host-based monitoring mechanisms] at [Assignment: organization-defined information system components].

| SI-4 (23) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SI-4(23)-1: OSSEC HIDS (Host Based Intrusion Detection Systesm) agent | |
| Parameter SI-4(23)-2: managed server operating systesms | |
| 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 (23) What is the solution and how is it implemented? |
| --- |
| Servers hosting proprietary operating systems (appliances) may not permit additional agent installation due to licensing and support agreements. In this event, the operating system is configured to transmit raw log data to the SIEM via syslog protocol. |

#### SI-4 (24) Control Enhancement (H)

The information system discovers, collects, distributes, and uses indicators of compromise.

| SI-4 (24) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (24) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### 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 | Click or tap here to enter text. |
| Part d | Click or tap here to enter text. |

#### SI-5 (1) Control Enhancement (H)

The organization employs automated mechanisms to make security alert and advisory information available throughout the organization.

| SI-5 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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 (1) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SI-6 Security Functionality Verification (M) (H)

The information system:

1. Verifies the correct operation of [Assignment: organization-defined security functions];
2. Performs this verification [FedRAMP Assignment: to include upon system startup and/or restart at least monthly];
3. Notifies [FedRAMP Assignment: to include system administrators and security personnel] of failed security verification tests; and
4. [Selection (one or more): shuts the information system down; restarts the information system; [FedRAMP Assignment: to include notification of system administrators and security personnel] when anomalies are discovered.

| SI-6 | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SI-6(a): Parameter SI-6(a): organization-defined security functions:; Monitor the integrity of system binaries, configuration files and log files; Prevention of malicious code; Permit only explicitly authorized network traffic | |
| Parameter SI-6(b): to include upon system startup and/or restart as well as at least monthly | |
| Parameter SI-6(c): to include system administrators and security personnel | |
| Parameter SI-6(d)-1: shuts the information system down; restarts the information system | |
| Parameter SI-6(d)-2: to include notification of system administrators and 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-6 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Prevention of malicious code: The GDIT Cloud Border Guard IDS devices monitor all Internet traffic to the GDIT Cloud, as well as Intrusion Detection and Prevention devices that monitor all traffic that passes through the GDIT Cloud firewalls. All traffic that generates an alert is forwarded to GDIT Cloud MMS SIEM for investigation and review in accordance with the controls outlined in SI-4: Signatures of malicious code. GDIT MMS HIDS also provides malicious code protection. Permit only explicitly authorized network traffic: The GDIT Cloud Border Guard firewalls, which are configured in a default deny-all policy. Any traffic that is allowed is explicitly configured to do so. All firewall logs are sent to GDIT Cloud MMS SIEM for review. At system startup, security functions are verified operationally that security events are being received by Traverse and subsequently, by AlienVault. Failure in these two verification processes will cause a restart to occur until such time as the security functions are operational. |
| Part b | The SIEM solution continually monitors system events from systems outlined in section 8.2 under “SIEM” to ensure only authorized network traffic is traversing the network. |
| Part c | The Engineers have configured systems to reboot automatically when the system is unable to send logs to the SIEM. Traverse will send an alert of the reboot to the NOC as an Event ticket in Cherwell. The Event ticket will initiate an investigation of why the system rebooted. |
| Part d | Security functions perform specific tasks on a routine basis. Verification of those specific tasks is done by security analysts. Failure of any of these tasks to perform will result in analysts determining that security function is not operational and requires remediation. |

### SI-7 Software & Information Integrity (M) (H)

The organization employs integrity verification tools to detect unauthorized changes to [Assignment: organization-defined software, firmware, and information].

| SI-7 | Control Summary Information |
| --- | --- |
| Responsible Role: Network Engineers | |
| Parameter SI-7: 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 | |

| SI-7 What is the solution and how is it implemented? |
| --- |
| The alerts from these tools are fed to GDIT Cloud MMS SIEM for Security Analysts to review. |

#### SI-7 (1) Control Enhancement (M) (H)

The information system performs an integrity check of [Assignment: organization-defined software, firmware, and information] [FedRAMP Selection (one or more): at startup; at [FedRAMP Assignment: to include security-relevant events]; [FedRAMP Assignment: at least monthly]].

| SI-7 (1) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineer | |
| Parameter SI-7(1)-1: organization-defined software, firmware, and information | |
| Parameter SI-7(1)-2: at startup | |
| Parameter SI-7(1)-3: 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 | |

| SI-7 (1) What is the solution and how is it implemented? |
| --- |
| In addition to the standard boot integrity checks, the Security Engineer employs the Tripwire File Integrity monitor to measure any change to the integrity of the system. For Windows hosts, this includes more than 90- critical system services, more than 100 system directories and their recursive files and binaries, more than 125 registry keys and their recursive sub keys, and the systems Resultant Set of Policy (RSOP) for the operating system. For file integrity checking, Tripwire hashes all files under monitoring and establishes a baseline for each file. Tripwire then re-checks the hash of that file to ensure it matches. If the hash does not match, Tripwire trips an alert. Tripwire conducts similar measurements of services, system directory, and configuration files on all Red Hat systems. Tripwire also measures network, storage, and virtualization equipment base configurations for change in a similar manner. Tripwire compares each of these measurements against identified baselines and alerts when a deviation is measured. In the event an alert is tripped, the Security Analyst opens a Cherwell Event to determine if a change was authorized or not. |

#### SI-7 (2) Control Enhancement (H)

The organization employs automated tools that provide notification to [Assignment: organization- defined personnel or roles]] upon discovering discrepancies during integrity verification.

| SI-7 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SI-7 (2): Click or tap here to enter text. | |
| 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-7 (2) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-7 (5) Control Enhancement (H)

The information system automatically [Selection (one or more): shuts the information system down; restarts the information system; implements [Assignment: organization-defined security safeguard]] when integrity violations are discovered.

| SI-7 (5) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| Parameter SI-7 (5): Click or tap here to enter text. | |
| 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-7 (5) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

#### SI-7 (7) Control Enhancement (M) (H)

The organization incorporates the detection of unauthorized [Assignment: organization-defined security-relevant changes to the information system] into the organizational incident response capability.

| SI-7 (7) | Control Summary Information |
| --- | --- |
| Responsible Role: Security Engineers | |
| Parameter SI-7 (7): unauthorized access or use of the system | |
| 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-7 (7) What is the solution and how is it implemented? |
| --- |
| When notified of unauthorized access by the GDIT Cloud MMS SIEM, such as modification of critical files, or alert from HIDS, Security Analysts will take ownership of the incident, create a Ticket in GDIT Cloud MMS Ticketing system and notify the GDIT Cloud security team to investigate and remediate. Upon resolution, the GDIT Cloud security team generates a post mortem After Action Report with root cause analysis. See The GDIT Cloud Incident Response Plan. |

#### SI-7 (14) Control Enhancement (H)

The organization:

1. Prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and
2. Provides exceptions to the source code requirement only for compelling mission/ operational requirements and with the approval of the authorizing official.

| SI-7 (14) | Control Summary Information |
| --- | --- |
| Responsible Role: Click or tap here to enter text. | |
| 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-7 (14) What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SI-8 Spam Protection (M) (H)

The organization:

1. Employs spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and
2. Updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policies and procedures.

| SI-8 | 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 | |

| SI-8 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | System administrators deploy a GDIT Cloud MMS email protection SMTP messaging gateway that provides inbound and outbound messaging security, with effective and accurate real-time anti-spam and antivirus protection, advanced content filtering, data loss prevention, and email encryption. |
| Part b | When new updates are available, the changes to the system are governed by the change process specified in the GDIT Cloud Change Management Process and Procedures Guide. Spam protection updates are categorized as a “standard change,” and are consequently pre-approved (for a period of time) and can be deployed during designated deployment windows. |

#### SI-8 (1) Control Enhancement (M) (H)

The organization centrally manages spam protection mechanisms.

| SI-8 (1) | 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 | |

| SI-8 (1) What is the solution and how is it implemented? |
| --- |
| System administrators centrally manage spam protection mechanisms by deploying a GDIT Cloud MMS email protection SMTP messaging gateway that provides inbound and outbound messaging security, with effective and accurate real-time anti-spam and antivirus protection, advanced content filtering, data loss prevention, and email encryption. |

#### SI-8 (2) Control Enhancement (M) (H)

The organization automatically updates spam protection mechanisms.

| SI-8 (2) | Control Summary Information |
| --- | --- |
| Responsible Role: Network 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 | |

| SI-8 (2) What is the solution and how is it implemented? |
| --- |
| GDIT Cloud MMS email protection messaging gateways (Zimbra and Spam Assassin) are configured to receive updates from Global Intelligence Networks. These are available as determined by the vendor. In addition threat information is received daily for ClamAV and Symantec to identify malicious code threats in email and attachments. |

### SI-10 Information Input Validation (M) (H)

The information system checks the validity of [Assignment: organization-defined information inputs].

| SI-10 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrators | |
| Parameter SI-10: Portal inputs | |
| 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-10 What is the solution and how is it implemented? |
| --- |
| Click or tap here to enter text. |

### SI-11 Error Handling (M) (H)

The information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and
2. Reveals error messages only to [Assignment: organization-defined personnel or roles].

| SI-11 | Control Summary Information |
| --- | --- |
| Responsible Role: System Administrator | |
| Parameter SI-11(b): Authorized system 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 | |

| SI-11 What is the solution and how is it implemented? | |
| --- | --- |
| Part a | Customers are responsible for protecting user name and password combinations; attributes used to validate a password reset request (e.g. security questions); personally identifiable information (excluding unique user name identifiers provided as a normal part of a transactional record); biometric data or personal characteristics used to authenticate identity; sensitive financial records (e.g. account numbers, access codes); content related to internal security functions (i.e., private encryption keys, white list or blacklist rules, object permission attributes and settings). |
| Part b | The GDIT Cloud network, compute components, and storage components are all configured to send SNMP traps and syslog data to GDIT Cloud MMS SIEM consequently, errors would either be written to the local disc (such as core dumps) where they are accessible by System Administrators, or sent to GDIT Cloud Ticketing system where they are accessible by all GDIT Cloud Staff. |

### 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? |
| --- |
| Audit data |

### SI-16 Memory Protection (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 Authorization | |

| SI-16 What is the solution and how is it implemented? |
| --- |
| 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. Attachment File Naming Convention 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. Attachment File Naming Convention. (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 an Information Security Policies and Procedures 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 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.

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 ‑. Information System Name and Title

| Unique Identifier | Information System Name | Information System Abbreviation |
| --- | --- | --- |
| Enter FedRAMP Application Number. | 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

GDIT has assessed the potential risk from Digital Identity errors, or Digital Identity misuse, related to a user’s asserted identity. GDIT 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 GDIT has identified that they support the Digital Identity Level that has been selected for the GDIT Cloud IaaS 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 GDIT.

Table 15‑6. Information System Name; Privacy POC

| Name | Peter Harroun |
| --- | --- |
| Title | Privacy Official's Point of Contact |
| CSP / Organization | General Dynamics Information Technology |
| Address | 11400 Westmoor Circle Suite 2501 Westminster CO 80021 US |
| 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

GDIT 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 GDIT can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

#### Qualifying Questions

|  |  |
| --- | --- |
| Select One | 1. Does the ISA collect, maintain, or share PII in any identifiable form? |
| Select One | 1. Does the ISA collect, maintain, or share PII information from or about the public? |
| Select One | 1. Has a Privacy Impact Assessment ever been performed for the ISA? |
| Select One | 1. 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 IaaStem 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 2‑1. 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 controls.

AC-5 Separation of Duties (M) (H) Additional FedRAMP Requirements and Guidance

1. FedRAMP Laws and Regulations

The Table 15‑8 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.