Cover Page

Policy Title	Policy and Procedures for Segregation of Duties in System User Roles
Document Identifier	PPM/SOD/2025
Previous title (if any)	Atlas User Profiles and Global Directory Application Guide
Policy objective	Provide information on minimum standards and offer guidance with respect to separation of duties.
Target audience	All UNFPA personnel
Risk control matrix	Control activities that are part of the process are detailed in the Risk Control Matrix
Checklist	N/A
Effective date	8 January 2025
Revision History	Issued: 8 January 2025
Mandatory review date	8 January 2028
Policy owner unit	Division for Management Services
Approval	Link to signed approval template

POLICY AND PROCEDURES FOR SEGREGATION OF DUTIES IN SYSTEM USER ROLES

TABLE OF CONTENTS

I. Purpose

1. The purpose of this policy is to outline the key segregation of duties principles and related controls in the UNFPA system role and access management process.

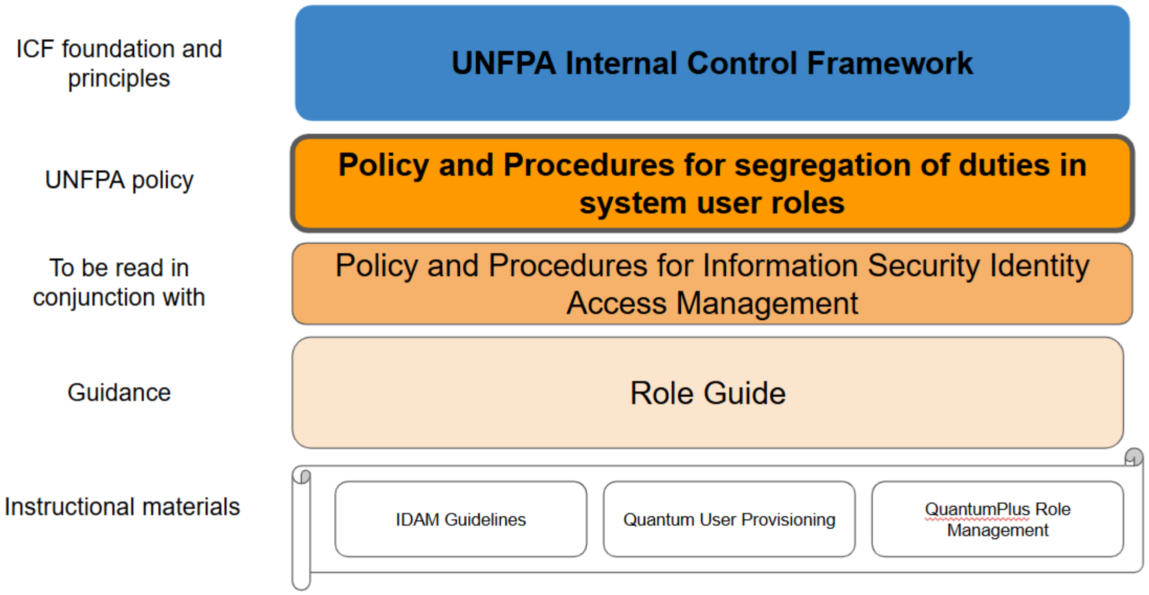
2. Segregation of duties is an internal control aimed at ensuring that no UNFPA personnel has the ability to control all phases of a process, sub-process or key transaction. A proper segregation of duties is a powerful tool to mitigate the risk of errors and wrongdoing, including fraud.

3. User role and access management is the process of provisioning system user roles based on a need-to-have basis to allow UNFPA personnel to perform their duties in an efficient, effective, and controlled manner.

4. The scope of this policy covers the user roles (business profiles and supplemental functions) in UNFPA's ERP and partners systems.

5. The present policy is part of a broader suite of policy and guidance documents. The below figure illustrates the relationship between these documents and contains links to each.

Overview: Policy and Guidance on Segregation of Duties


ICF foundation and principles
UNFPA Internal Control Framework
UNFPA policy
Policy and Procedures for segregation of duties in system user roles
To be read in conjunction with
Policy and Procedures for Information Security Identity Access Management
Guidance
Role Guide
Instructional materials
IDAM Guidelines
Quantum User Provisioning
QuantumPlus Role Management

II. Policy

6. This policy establishes the key segregation of duties principles that need to be followed by UNFPA managers when assigning system rights to the personnel in their office, identifies control actions to mitigate potential risks related to the process and establishes the following.

7. Segregation of duties is achieved by assigning different tasks to different individuals and ensuring that high risk and high materiality activities are reviewed by a second individual with the right seniority and expertise (four-eyes principle). This is true for all processes and all activities performed in the system or outside the system.

8. In assigning system rights, heads of unit[1] are responsible for ensuring that roles assigned are adequate to the individual's responsibilities, expertise, functional position, seniority, and contractual modality and that they cannot control all phases of a process, sub-process or key transaction.

9. Heads of units must review system access entitlements for their office on a regular basis (not less than annually, and when significant changes occur in the staffing and/or organizational structure of the office) and certify that user assignments are up to date following the procedures outlined below.

10. The head of unit must follow these key principles of segregation of duties when assigning system rights:

    10.1. An individual cannot control all phases of a process, sub-process or key transaction.

    10.2. Finance and Procurement profiles cannot be combined.

    10.3. Roles allowing creation (Buyer) and approval (Manager PO) of purchase orders[2] cannot be combined.

    10.4. Roles allowing receipts of goods (Receiver) cannot be combined with roles allowing creation or approval of purchase orders.

    10.5. Roles allowing approval of requisitions[3] (Requisition Manager) cannot be combined with roles allowing creation or approval of purchase orders.

[1] The UNFPA head of unit refers to the representative, division director, regional or subregional director, country director or the Chief of Operations (or the delegated officer), as appropriate.

[2] In UNFPA's ERP system, Purchase Orders are referred to as Obligations. The two definitions can be used indistinctively.

[3] In UNFPA's ERP system Requisitions are referred to as Commitments. The two definitions can be used indistinctly.

11. Combinations of roles which violate the above principles are referred to as segregation of duties conflicts. The complete list of conflicts is documented in the System Role Guide.

12. In exceptional circumstances, an office may need to request a combination of system roles that is not allowed by the system. This is an Internal Control Framework (ICF) exception and must be approved by the ICF Team in the Division for Management Services (DMS).

13. Exceptions expose the organization to a higher level of risk and, hence, must be requested only when absolutely necessary. Before requesting an exception, each office needs to consider any possible alternative, including revising the internal division of labor and/or requesting support from other offices and/or the regional office.

14. Heads of unit are responsible for managing and monitoring the risk exposure resulting from activities undertaken by users with conflicting roles and by power-users. Power-users are the administrators and other personnel who are entrusted with special rights to allow support, troubleshooting, and review and correction of certain transactions. The system rights entrusted to these individuals span over multiple business units, provide access to sensitive data, and the activities they are allowed to perform inherently carry high risks.

15. The ICF Team independently reviews the roles assigned and the exceptions granted on an annual basis.

III. Procedures

A. System Roles

16. UNFPA personnel can refer to the system role guide for a comprehensive list of roles. The role guide contains a description of each business profile and supplemental function. Its purpose is to facilitate the submission and approval of user provisioning requests.

B. User Access Management

17. The user provisioning process is described in the Policy and Procedures for Information Security Identity Access Management.

18. Access to Quantum is managed through the Identity and Access Management System (IDAM) and detailed guidance is contained in the Quantum Resource Center.

19. Access to QuantumPlus is managed through a self-service application and detailed guidance is contained in the QuantumPlus user guides and training material pages.

C. Preventative Controls

20. Key segregation of duties conflicts are prevented by the system, meaning they are not available for provisioning.

21. It is important to note that, while combinations of conflicting roles are not allowed by the system, the system cannot replace management judgment in assigning the right roles to the right individuals.

D. Detective Controls

22. On a regular basis, heads of unit are required to review system access entitlements for their office and certify that they are updated and relevant.

23. During this exercise all profiles and functions that are no longer used or needed will have to be removed through a regular user provisioning request[4].

24. The certification process is managed by the Information Technology Solutions Office (ITSO) with DMS as business owner of the process.

25. On an annual basis the ICF Team performs an independent review of the roles across the organization with focus on the roles that carry higher risk and on the exceptions granted during the year.

E. Management of Exceptions

26. There may be occasions where an office needs to request a combination of Quantum roles that is not allowed by the system. This must be requested and approved outside of the system through a Global Service Desk request using the category Quantum Access Management ICF/SOD requests for exceptions.

27. Each request for exception must be supported by proper information and justification. It must clearly indicate: the profiles and functions requested, the rationale (why is it needed and why the need cannot be addressed through a standard combination of roles), the timeline (exceptions are usually time-bound), and the mitigating controls introduced to manage the risk. The request must be approved in writing by the head of unit.

[4] User provisioning procedures for Quantum and QuantumPlus are documented in the instructional material referenced in the overview table.

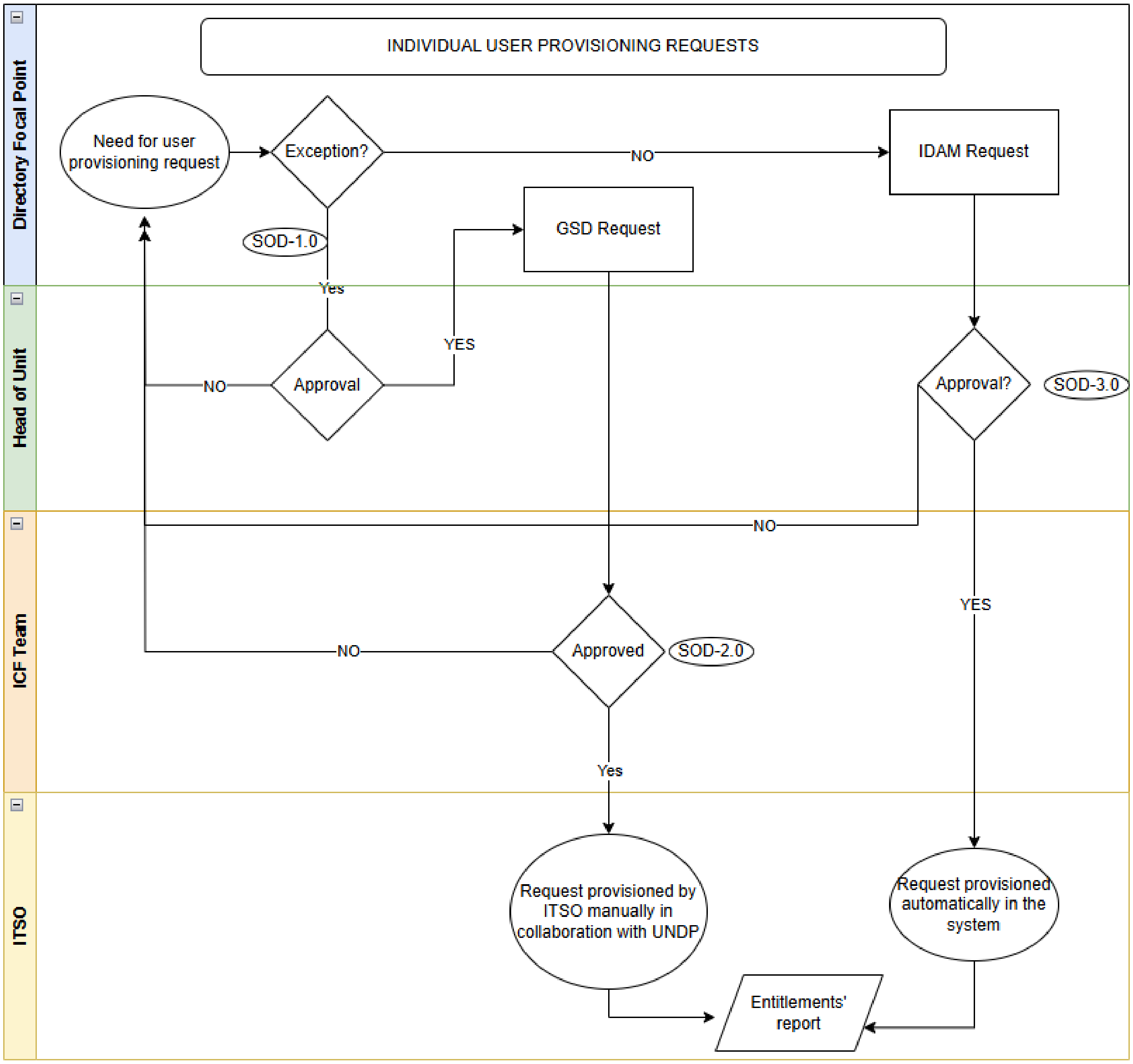
F. Users with Special Privileges and Power-user Accounts

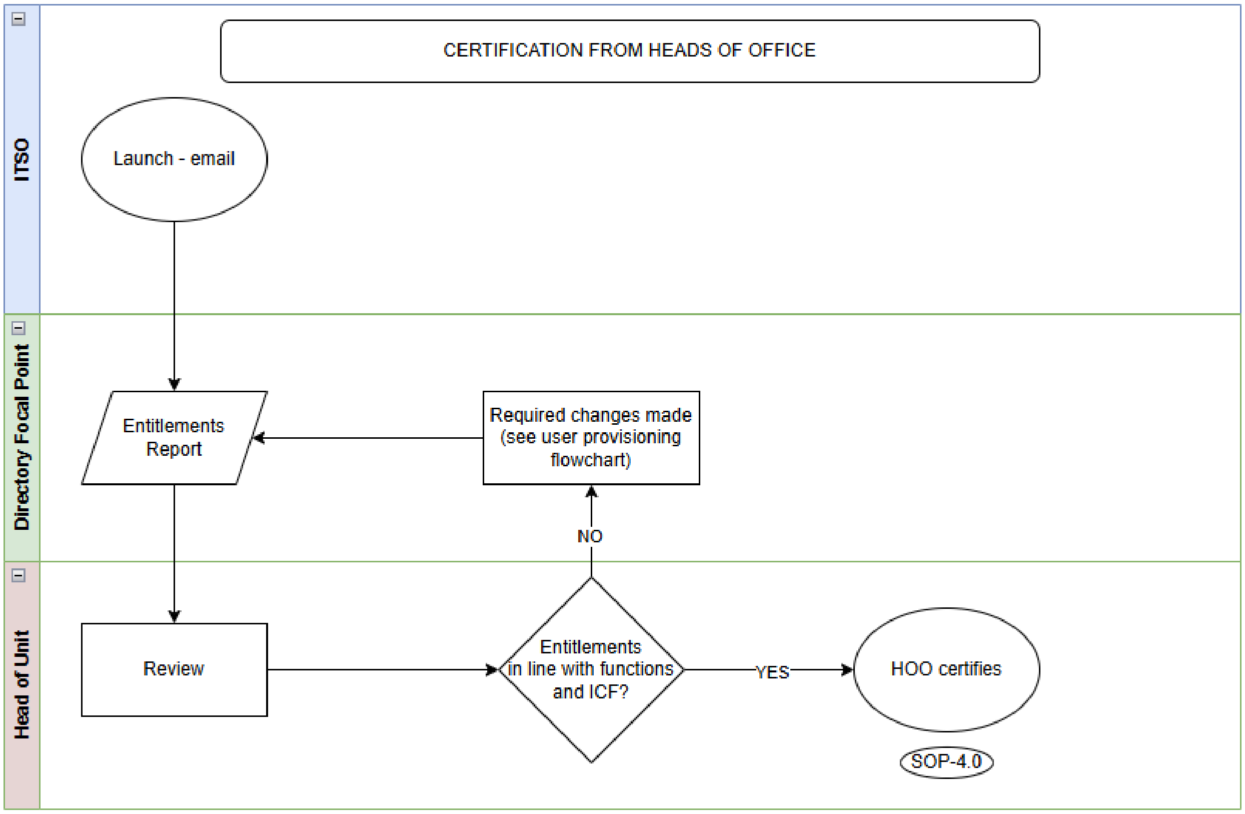
28. Heads of unit must follow the Policy and Procedures for Information Security Identity Access Management to request privileged accounts to be created for those staff in their departments that require elevated access to Quantum. These accounts are separate from their regular Quantum accounts. The Director of ITSO will approve the creation of these privileged accounts based on a written request from the respective head of unit. In the case of Quantum, there are basic User Audit reports that may be used in monitoring the usage of account activity.

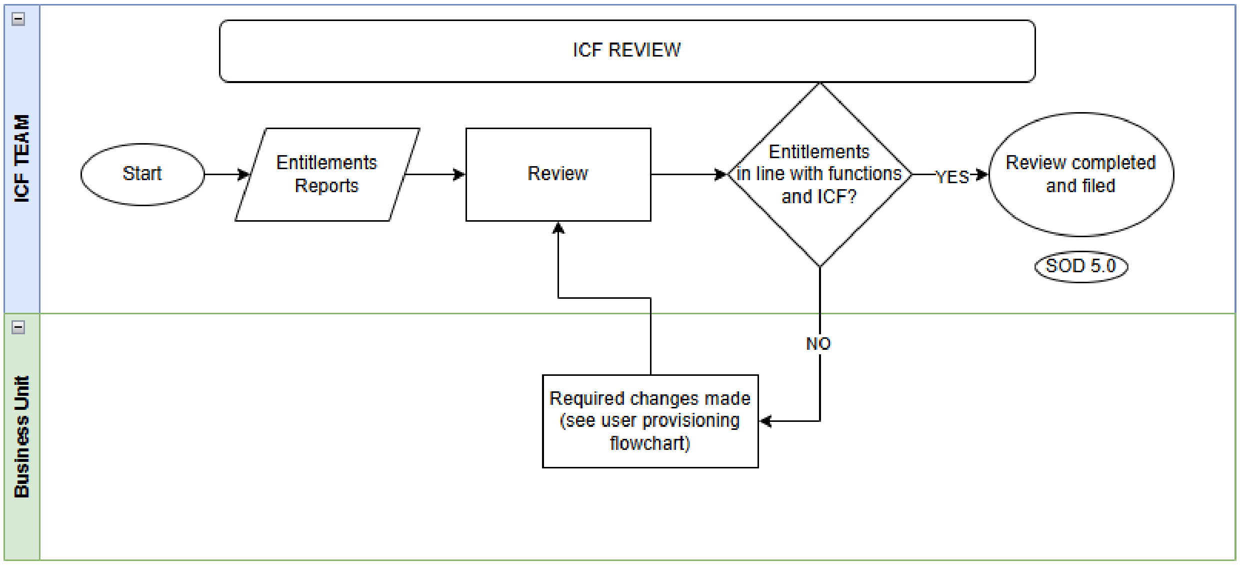
IV. Other

29. No other content available.

V. Process Overview Flowchart(s)


Directory Focal Point
Head of Unit
ICF Team
ITSO
INDIVIDUAL USER PROVISIONING REQUESTS
Need for user provisioning request
Exception?
NO
IDAM Request
SOD-1.0
GSD Request
Yes
YES
NO
Approval
Approval?
SOD-3.0
NO
YES
NO
Approved
SOD-2.0
Yes
Request provisioned by ITSO manually in collaboration with UNDP
Request provisioned automatically in the system
Entitlements' report


ITSO
Directory Focal Point
Head of Unit
CERTIFICATION FROM HEADS OF OFFICE
Launch - email
Entitlements Report
Required changes made (see user provisioning flowchart)
NO
Review
Entitlements in line with functions and ICF?
YES
HOO certifies
SOP-4.0


ICF TEAM
Business Unit
ICF REVIEW
Start
Entitlements Reports
Review
Entitlements in line with functions and ICF?
YES
Review completed and filed
SOD 5.0
NO
Required changes made (see user provisioning flowchart)

VI. Risk Control Matrix

Risk Description	First Line of Defense Controls			Second Line of Defense Controls		
	Control Activity Description	Reference	Who performs	Control Activity Description	Reference	Who performs
Users are provisioned with SoD conflicts by mistake or purposely by the Directory Focal Point (DFP).	The system automatically prevents conflicting profiles and functions to be provisioned	SOD 1.0	Automated Control (IDAM)	N/A	N/A	N/A
ICF/SOD exceptions are granted without approval of the ICF team	All ICF/SOD exceptions are managed through GSD. The workflow requires approval by the ICF Team (who verifies that the request is justified and approved by the head of unit) before being processed by ITSO.	SOD 2.0	ICF Team	On an annual basis the ICF team reviews the entitlements in the system to verify that all exceptions are valid and relevant.	SOD 5.0	ICF Team
System access rights are granted without the approval of the head of unit and/or are not consistent with the individual's responsibilities, expertise, functional position, seniority, and contractual modality	System access rights are provided to the right individuals based on a need-to-have basis, ensuring that roles assigned are adequate to the individual's responsibilities, expertise, functional position, seniority, and contractual modality	SOD 3.0	Head of unit	On an annual basis the head of unit reviews the entitlements in the system and certify that they are still relevant and adequate exceptions are valid and relevant and adequate to the individual's responsibilities, expertise, functional position, seniority, and contractual modality.	SOD 4.0	Head of unit

- - END - -