Administrative Management Manual

Odoo Implementation Guide

Prepared by: Axon System

Date: November 24, 2025

Contents

List of Figures

List of Tables

Part I

The Strategic Foundation

Chapter 1

The TAO of Odoo Administrative Management: Guiding Philosophy

Odoo Administrative Management is more than a utility for organizing records—it is the foundational architecture that ensures your organization operates with clarity, consistency, and control. At its core lies the disciplined stewardship of master data and the seamless flow of information across systems. This chapter explores the guiding philosophy that shapes how Odoo approaches administrative integrity: not as a static back-end chore, but as a dynamic, strategic enabler of operational excellence.

1.1 The Core Philosophy: A Unified Administrative Nervous System

In Odoo, administrative management functions as your organization's data nervous system constantly synchronizing identities, structures, and definitions that give meaning to every business process. Unlike legacy systems where master data is fragmented across spreadsheets, siloed databases, and disconnected tools, Odoo embeds administrative coherence into every module by design.

Customer records, product catalogs, employee profiles, chart of accounts, tax rules, and warehouse locations are not isolated entries—they are interconnected master data entities that serve as the single source of truth for sales, procurement, inventory, accounting, HR, and beyond.

Every new product created, every customer imported, every supplier updated flows instantly into all dependent workflows—without manual duplication or reconciliation. This eliminates data drift, reduces governance risk, and ensures that decisions across the organization are based on consistent, reliable information.

This unity transforms administrative work from a maintenance burden into a real-time strategic asset, empowering teams to operate with confidence, agility, and precision.

Key Takeaway: In Odoo, data integrity doesn't happen *after* operations—it is the *foundation* of operations.

1.2 Guiding Principles: Consistency, Interoperability, and Governance

Odoo Administrative Management is built on three interlocking principles that define its approach to master data and data exchange:

Consistency

Master data must be uniform, accurate, and unambiguous across all contexts. Odoo enforces this through:

- Centralized definition of core entities (e.g., Customers, Products, Employees, Accounts)
- Validation rules that prevent duplicates, malformed entries, or conflicting configurations
- Real-time synchronization: updating a customer's address in one place updates it everywhere—sales orders, invoices, delivery slips, and contracts

Interoperability Data must flow freely into and out of Odoo—without requiring custom scripts or fragile manual exports. Odoo ensures seamless data exchange through:

- Native, intelligent import/export tools with template-guided mapping
- Support for CSV, Excel, and XML formats with automatic field recognition
- Built-in data matching logic (e.g., "Update existing records if email matches")
- API-first architecture for integration with external systems (ERP, CRM, e-commerce, HRIS)

Governance As organizations scale, data must be managed with clear ownership, version control, and auditability. Odoo embeds governance into daily operations:

- Role-based access controls that restrict who can create, edit, or delete master records
- Immutable change logs that track who modified what and when
- Data validation workflows (e.g., "New vendor requires manager approval")
- Multi-company data isolation with optional shared master records

Together, these principles ensure that Odoo Administrative Management is not just a repository of records—but a living framework for data trust, enabling scalable, compliant, and efficient operations.

1.3 Frame of Reference: Master Data as the Spine of the Business Ecosystem

In the Odoo ecosystem, master data is the invisible spine that aligns every business function. Poorly managed data causes cascading errors: incorrect pricing, failed deliveries, compliance gaps, and financial misstatements. Odoo treats master data as mission-critical infrastructure:

- A product record defines not only SKU and description but also costing method, tax category, warehouse rules, and e-commerce visibility—impacting inventory, accounting, sales, and logistics simultaneously.
- A customer record carries payment terms, fiscal position, shipping preferences, and communication history—shaping invoicing, collections, and service delivery.
- An employee profile links HR data with project assignments, expense policies, and approval hierarchies—enabling automated workflows across departments.
- Even chart of accounts and tax templates are treated as master data, ensuring financial consistency across regions and legal entities.

This interconnectedness means that high-quality master data directly translates into operational reliability and strategic insight.

By placing administrative management at the center, Odoo enables:

- **End-to-end data integrity:** From onboarding a new vendor to reconciling their payments—every step uses the same trusted record.
- **Effortless onboarding and migration:** Bulk import tools with error previews and rollback options simplify data transitions during go-live or mergers.
- **Scalable standardization:** Global organizations can enforce data models centrally while allowing local teams controlled flexibility—without fragmentation.

In essence: Odoo Administrative Management doesn't just store data—it orchestrates truth.

Chapter 2

Strategic Context and Business Purpose

2.1 System Context (C4-Level 1):

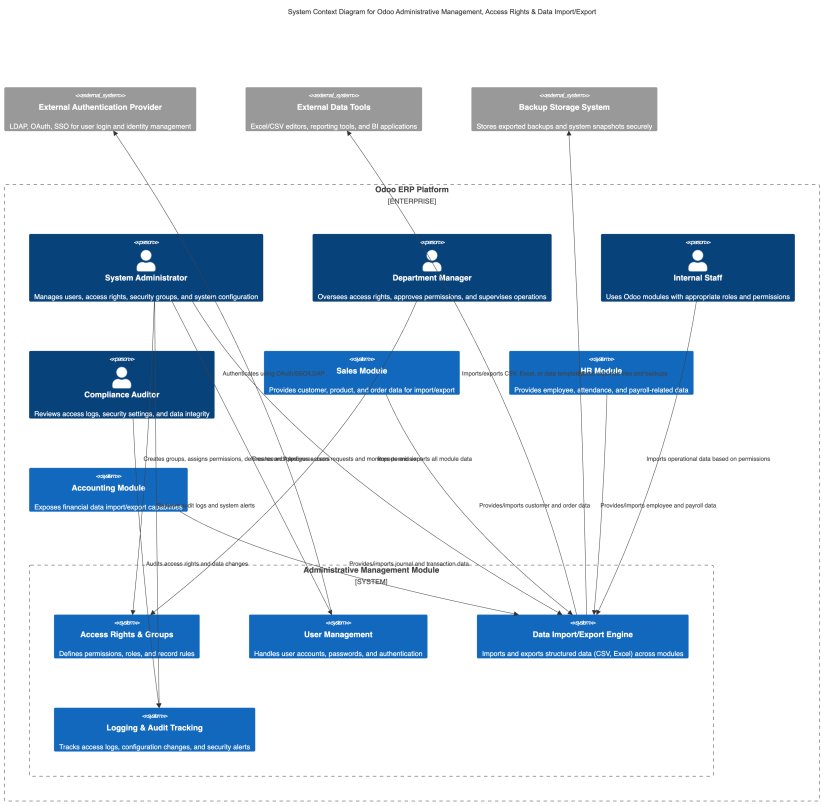

Figure 2.1: C1 Diagram: Odoo Administrative Management System Context

The C1 diagram illustrates the system context for Odoo's Administrative Management, Access Rights, and Data Import/Export functionalities. It shows how users and external systems interact with the core administrative components of the Odoo ERP Platform, with a particular focus on the roles of the System Administrator, Compliance Auditor, and the underlying modules that manage security, user data, and data exchange.

Interactions:

Users:

i. **System Administrator:** Manages all aspects of user accounts, access rights, security groups, and system configuration. Directly interacts with the User Management, Access Rights & Groups, and Logging & Audit Tracking modules. Also configures authentication with the External Authentication Provider.

ii. **Department Manager:** Oversees access rights and approves permission requests within their department. Interacts with the Administrative Management Module to monitor permissions and export data as needed.

iii. **Internal Staff:** Uses various Odoo modules (like Sales, HR) according to their assigned roles and permissions. Their operational data is imported into the system based on these permissions.

iv. **Compliance Auditor:** Reviews access logs, security settings, and data integrity. Interacts with the Logging & Audit Tracking module and the Access Rights & Groups module to audit changes and ensure compliance.

Internal Odoo Modules:

i. **Sales Module:** Provides customer, product, and order data. This data can be imported/exported via the Data Import/Export Engine, which is managed through the Administrative Management Module.

ii. **HR Module:** Provides employee, attendance, and payroll-related data. This data is also subject to import/export operations and is governed by the access rights defined in the Administrative Management Module.

iii. **Accounting Module:** Exposes its financial data for import/export capabilities. Its data flows through the Data Import/Export Engine, which is centrally managed by the Administrative Management Module.

iv. **Administrative Management Module:** This is the central system managing the other administrative sub-modules. It coordinates between User Management, Access Rights & Groups, and the Data Import/Export Engine. It provides the interface for Department Managers and System Administrators to perform their duties.

v. **Access Rights & Groups:** Defines the permissions, roles, and record rules that govern what data users can see and modify across all Odoo modules.

vi. **User Management:** Handles the creation, modification, and deletion of user accounts, including passwords and authentication methods.

vii. **Data Import/Export Engine:** A core component that facilitates the structured import and export of data (CSV, Excel) across all modules, acting as a conduit for data exchange between internal modules and external tools.

viii. **Logging & Audit Tracking:** Tracks all access logs, configuration changes, and security alerts, providing a critical audit trail for the Compliance Auditor and System Administrator.

External Systems:

i. **External Authentication Provider:** An external system (e.g., LDAP, OAuth, SSO) used for user login and identity management. The User Management module authenticates users against this provider.

ii. **External Data Tools:** Includes Excel/CSV editors, reporting tools, and BI applications. These tools interact bi-directionally with the Data Import/Export Engine to import data into Odoo or export data for analysis.

iii. **Backup Storage System:** A secure external system where exported backups and system snapshots are stored. The Data Import/Export Engine sends backup files to this system.

Dependencies:

i. **User Management & Authentication:** The entire system depends on the User Management module for creating and authenticating users, often relying on an External Authentication Provider for single sign-on.

ii. **Access Control Framework:** All modules depend on the Access Rights & Groups module to enforce security policies and ensure users only see and modify data they are authorized to access.

iii. **Data Import/Export Engine:** Critical for interoperability, this engine is depended upon by all modules for bulk data operations and integration with External Data Tools and the Backup Storage System.

iv. **Audit and Logging System:** The Logging & Audit Tracking module is a dependency for compliance and security, providing the necessary records for the Compliance Auditor and System Administrator to review system activity.

v. **Administrative Management Module:** Acts as the central orchestrator. Other administrative sub-modules (User Management, Access Rights, etc.) and user roles (System Admin, Department Manager) depend on it for coordinated operation.

Summary

This diagram highlights that the administrative backbone of the Odoo ERP Platform is centered around robust access control, secure user management, and flexible data exchange. The interactions show how different user roles leverage these administrative functions, while the dependencies underscore the critical infrastructure required for a secure, compliant, and interoperable system. The Accounting Module, while present, is depicted here not for its core financial functions, but for its role in exposing data for import/export under the governance of the administrative framework.

2.2 SIPOC Analysis: Mapping the Accounting Value Stream in Odoo

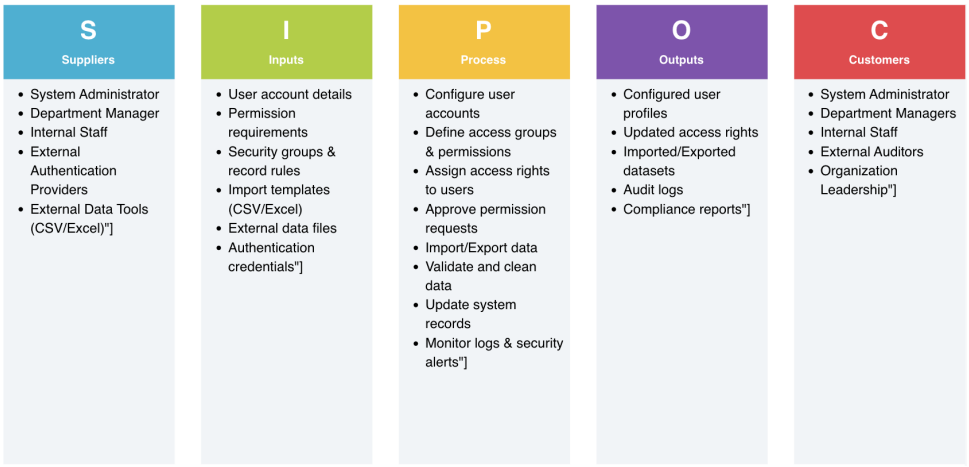

Figure 2.2: SIPOC Diagram: Odoo Administrative Value Stream

Detailed SIPOC Breakdown:

- **Suppliers:** These are the sources of administrative data and access-related information that feed into Odoo Administrative Management:
  - System administrators: Create users, define roles, manage security groups.
  - Department managers: Submit or approve permission requests.
  - Internal staff: Request access and submit data for import/export.
  - External authentication providers: Supply identity verification (OAuth, LDAP, SSO).
  - External data tools: Provide CSV/Excel datasets for import.
  - Odoo modules (Sales, HR, Accounting, Inventory, etc.): Provide structured data for import/export operations.
- **Inputs:** Key data and configurations required for effective administrative and access management:
  - User account details (email, role, department)
  - Access permission requirements
  - Security groups and record rules
  - Company permission and security policies
  - Import templates (CSV/Excel)
  - Data files for import (customer, employee, product, transaction data)
  - Export format preferences (CSV, XLSX)
  - Authentication credentials from SSO/OAuth/LDAP

  - Backup files and exported datasets

- **Process Steps:** Odoo automates and streamlines the following key administrative steps:

  1. Initial Configuration

     Define user roles, groups, password policies, authentication methods, and access rules.
  2. User Creation and Permission Setup

     Create user accounts, assign group memberships, configure access control lists (ACLs), and apply record rules.
  3. Permission Review and Approval

     Validate and approve permission changes requested by staff or required by departments.
  4. Data Import and Export

     Import structured data (CSV/Excel) and export datasets for reporting, backup, or migration.
  5. Data Validation

     Validate imported records, correct errors, and ensure data consistency before committing changes.
  6. System Monitoring and Audit Logging

     Track login activity, permission changes, configuration updates, and maintain audit logs for compliance.

- **Outputs:** Odoo produces reliable administrative outputs, including:

  - Configured and active user accounts
  - Updated access rights and permission matrices
  - Imported datasets stored in relevant Odoo modules
  - Exported datasets for reporting or integration
  - Audit logs and access trails
  - Permission change history
  - Security compliance and activity reports
  - Backup files and system snapshots

- **Customers:**

  - System administrators: Maintain user access and system integrity.
  - Department managers: Ensure staff have proper permissions for daily operations.
  - Internal staff: Rely on correctly assigned permissions to perform their tasks.
  - External auditors: Review logs and verify compliance.
  - Company leadership: Depend on secure and reliable access control.
  - IT/Security teams: Monitor identity management and system security.
  - Other Odoo users: Benefit from consistent and accurate access rights across modules.

2.3 The Pain-Gain Canvas: Problems Solved and Value Created by the Module

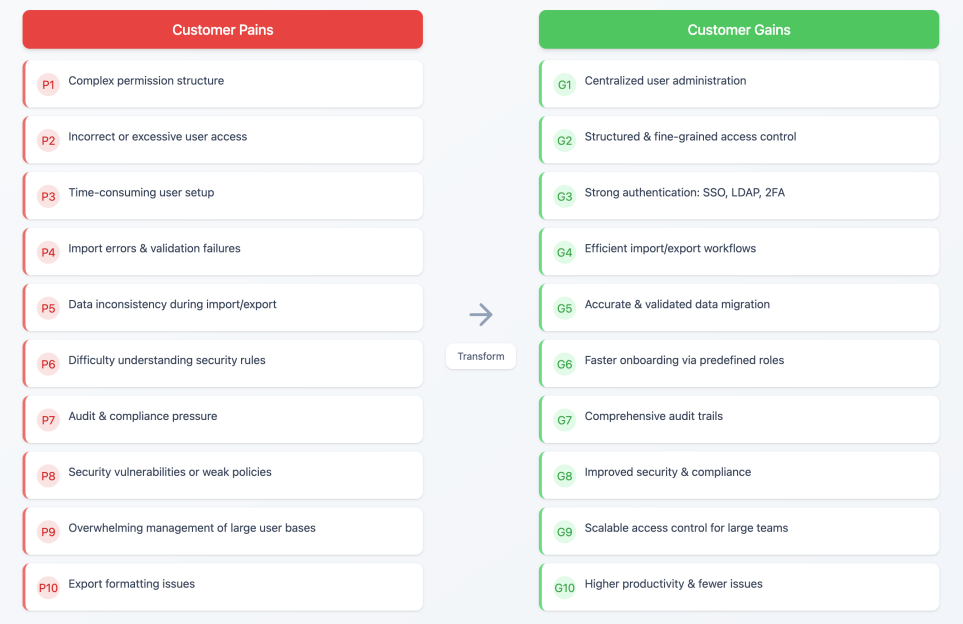

Figure 2.3: Pain-Gain Diagram: Odoo Administrative Value Proposition

Before Odoo	With Odoo
Managed user access manually with inconsistent rules	Centralized user management with clearly defined roles and groups.
Gave permissions individually to each employee	Assign permissions instantly through User Groups and Access Control Lists.
Difficult to control who can see or edit sensitive data	Record Rules ensure precise data visibility and secure access.
No audit trail for administrative changes	Full logs for user activity, configuration updates, and access changes.
Data import involved copying and pasting into multiple tools	Import CSV/XLSX files directly into any Odoo model.
Frequent data errors due to mismatched template formats	Pre-built templates and validation checks reduce import mistakes.
Exporting data required manual formatting	One-click export to spreadsheet-ready formats.
Bulk updates required editing each record individually	Mass editing and batch operations available across all modules.

Part II

Architectural and Conceptual Framework

Chapter 3

Architectural Blueprint: Components and Containers

3.1 Defining a "Container" in the Odoo Context

Within Odoo's Administrative Management, Access Rights, and Data Import/Export framework, the term "container" is not an official technical component. However, the concept can be applied informally to describe the structures Odoo uses to organize, secure, and transport administrative and data-related elements. In this context, a "container" refers to an Odoo object or configuration entity that groups users, permissions, or datasets into manageable units.

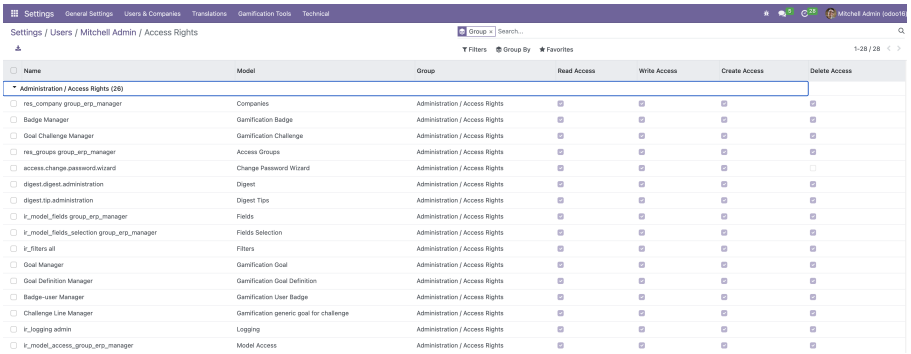

Figure 3.1: User Groups as Containers in Odoo Administration

1. **User Groups (Access Control Container):**

   User groups serve as the primary container for managing access rights. They allow administrators to bundle permissions and assign them to multiple users efficiently. Each group aggregates:

   - Access Control Lists (ACLs)
   - Record Rules
   - Menu visibility settings
   - Application-level permissions

   Use Case: Users in the "Inventory Manager" group automatically receive permissions for warehouse adjustments, transfers, and reporting, without being configured individually.

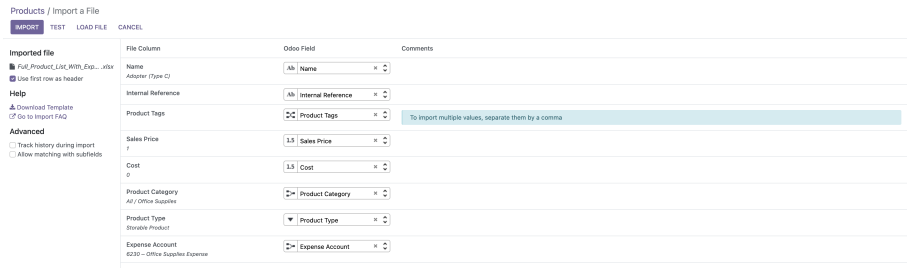

Figure 3.2: Models as Data Containers for Import/Export

2. **Models (Data Storage Containers):**

   In Odoo, each model acts as a container for a specific category of business data—customers, products, invoices, employees, etc. During import or export operations, the model defines:

   - Available fields
   - Required columns
   - Data structure and validation rules

   Use Case: Importing customer records uses the `res.partner` model as the container that holds all partner-related fields such as name, address, email, and VAT number.

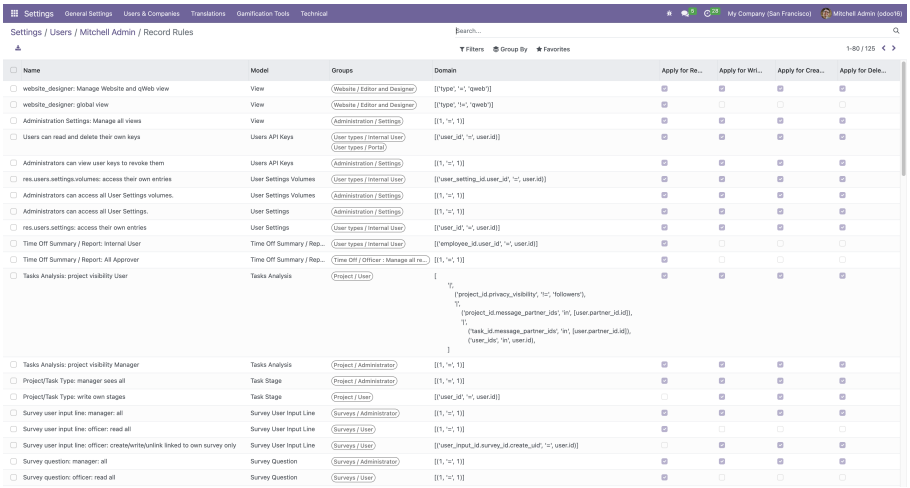

Figure 3.3: Record Rules as Containers for Data Visibility

3. **Record Rules (Visibility Containers):**

   Record rules act as rule-based containers that define which subset of records a user or group can access. These rules enforce:

   - Row-level security
   - Multi-company data separation
   - Department-based restrictions

   Use Case: A sales representative sees only their own customers due to a record rule restricting access based on the “assigned user” field.

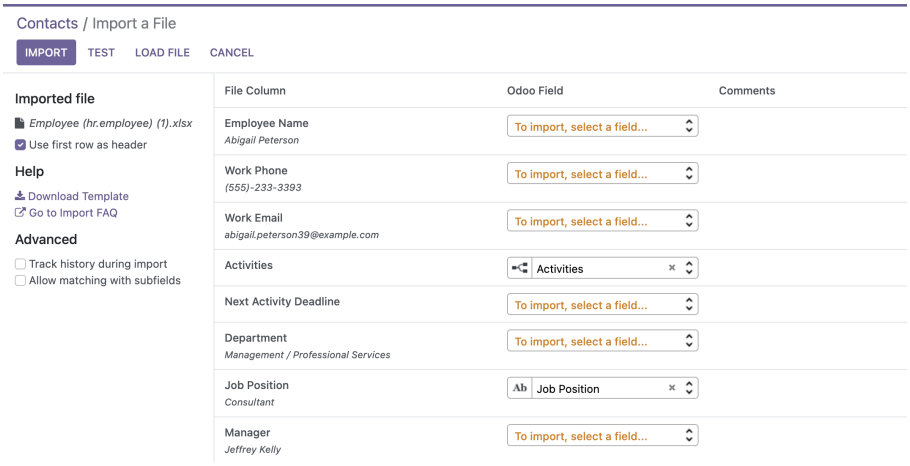

Figure 3.4: Import/Export Templates as Data Transfer Containers

4. **Import/Export Templates (Data Transfer Containers):**

   Templates used for importing or exporting data—typically CSV or XLSX—function as temporary containers that package structured information for transfer into or out of Odoo.

   These templates include:

   - Column mappings for model fields
   - Required identifiers (external IDs, names, emails, etc.)
   - Sample values for validation

   Use Case: A CSV file containing product inventory levels serves as a container that Odoo reads to update stock quantities.

5. **Company Environment (Multi-Entity Administrative Container):**

   In multi-company setups, each company acts as a container for its administrative and security configuration, including:

   - Users and access rights
   - Menu permissions
   - Data segregation rules
   - Import/export permissions

   Use Case: Employees of Company A cannot see the data of Company B because each company acts as its own administrative container enforced by record rules.

3.2 Identifying Key Containers: Odoo Server, Web Client, Security Engine, and Data Services

The C2 diagram highlights the technical architecture of Odoo Administrative Management and Data Import/Export by depicting its major containers and how they interact. The key

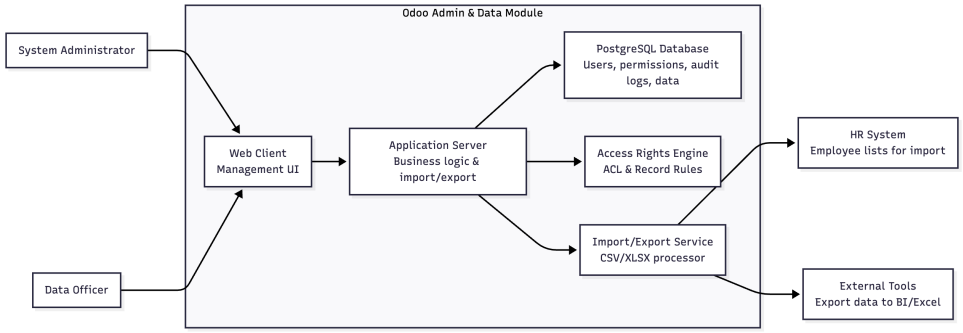

Figure 3.5: C2 Diagram

components include the Odoo Server, the PostgreSQL database, the Web client, the Access Rights Engine, and the Import/Export Service. Together, they form the system's runtime and administrative data-processing environment.

At the core lies the Odoo Server, built using Python for business logic and XML for views and configuration. The server executes critical administrative tasks such as user creation, role assignment, permission enforcement, record rule evaluation, and audit logging. It also handles data import/export logic, validating incoming datasets and preparing data for structured export. The server manages all workflow logic and coordinates communication between the database, access control engine, and the user interface.

The PostgreSQL database serves as the persistent storage for all administrative and imported/exported data. This includes user accounts, group memberships, access rules, audit trails, and imported business records. The database ensures data integrity, maintains transaction consistency, and supports multi-company and multi-module data separation.

The Web client, developed using JavaScript/HTML, provides the front-end interface for system administrators and data officers. Users interact with the system to manage user accounts, configure access permissions, monitor audit logs, and upload or export data files. The web client communicates in real-time with the Odoo Server via RPC and REST calls to retrieve, validate, and submit administrative and import/export data.

The Access Rights Engine enforces all security policies and evaluates permissions in real-time, ensuring users see and modify only authorized records. Meanwhile, the Import/Export Service processes structured CSV/XLSX files, performing validations, error reporting, and preparing datasets for export to external tools like BI systems or HR platforms. Together, these containers enable secure, efficient, and auditable administrative management within Odoo.

3.3 Mapping the Core Components of Odoo Administrative Management and Data Import/Export

Odoo Administrative Management and Data Import/Export is a robust, secure, and user-friendly system designed to streamline user administration, access control, security manage-

ment, and bulk data operations. Understanding its core components is essential for efficient setup, configuration, and daily administration. Below is an overview of the main elements that constitute this system:

1. **User Management and Groups**

   Centralized administration of users and roles. Define groups for access control (e.g., administrators, finance managers, data officers). Assign multiple users to groups to simplify permission management. Supports multi-company setups with isolated user domains.

2. **Access Rights and Record Rules**

   Fine-grained permission system based on groups and rules. Access Control Lists (ACLs) define CRUD rights for models. Record rules enforce row-level security, restricting records visible to users based on roles, departments, or companies. Audit-ready configuration ensures compliance with internal policies.

3. **Web Client Interface**

   Provides an intuitive interface for managing users, roles, permissions, and audit logs. Supports real-time interaction with the server for administrative tasks. Enables data officers to upload, validate, and export datasets using CSV/XLSX templates.

4. **Import/Export Service**

   Handles bulk data transfer into and out of Odoo. Supports validation of imported datasets to prevent errors or duplicates. Predefined templates simplify importing employees, products, or transactional data. Exports structured data for use in external tools like BI platforms or spreadsheets.

5. **Security Engine**

   Evaluates and enforces ACLs, record rules, and multi-company restrictions. Ensures that users see and modify only the data they are authorized to access. Works in real-time with the server and web client for all administrative actions.

6. **Audit Trail and Logs**

   Tracks all administrative actions, including user creation, role changes, permission updates, and data imports. Provides transparent logs for internal reviews, compliance checks, and audits. Essential for accountability and monitoring.

7. **Database (PostgreSQL)**

   Persistent storage for user accounts, access rules, audit logs, and imported/exported data. Ensures data integrity, transactional consistency, and multi-company separation.

8. **Multi-Company and Multi-Environment Support**

   Isolates access and data per company or environment. Facilitates secure operations for organizations managing multiple legal entities. Ensures that imported data is correctly segregated by company or department.

9. **Configuration and Settings**

   Define system-wide administrative defaults, such as password policies, user roles, access levels, and record rule templates. Configure import/export templates, file formats, and validation rules. Control workflow and approval processes for sensitive administrative operations.

10. **Integration with Other Odoo Modules**

    Seamless interaction with Sales, Purchase, HR, Inventory, and Accounting modules. Enables automatic user role propagation and secure data import/export across modules.

Chapter 4

Ecosystem Integrations

4.1 Core Odoo Integrations for Administrative Management and Data Import/Export

Odoo's Administrative Management and Data Import/Export features are designed to integrate seamlessly with other Odoo modules and external systems. These integrations streamline user administration, secure data handling, and enable bulk data operations with minimal manual effort. Below are the key integrations that enhance administrative and data management functionality:

1. **User Management Across Modules**
    - Centralized Role Propagation: User roles and group memberships are automatically applied across Sales, Purchase, HR, Inventory, and other modules.
    - Cross-Module Access Enforcement: Permissions set in the admin module immediately reflect across all connected applications.
    - Automated Notifications: Users receive alerts when roles, permissions, or access rights are changed.
2. **Access Rights and Security Engine**
    - ACLs and Record Rules: Enforce CRUD and row-level access consistently across all modules.
    - Multi-Company Security: Ensures that users see only the data relevant to their company or department.
    - Audit Trail Integration: Logs all administrative actions for compliance, reporting, and review.
3. **Web Client Interface**
    - Centralized Admin Dashboard: Manage users, groups, access rights, and audit logs from a single interface.
    - Real-Time Updates: Changes to permissions, groups, or roles take effect immediately across all modules.
    - File Upload/Download: Upload import files or download exported datasets directly through the web client.

4. **Import/Export Service**
    - CSV/XLSX Templates: Preconfigured templates for importing employees, products, or transactional data.
    - Data Validation: Automatic error checks to ensure accurate imports and prevent duplicates.
    - External Tool Integration: Exports data for use in spreadsheets, BI platforms, or HR systems.
    - Bulk Operations: Enables mass updates, imports, and exports without manual record-by-record entry.
5. **Integration with HR and Payroll**
    - Employee Data Import: Syncs HR records for user creation and role assignment.
    - Payroll Data Management: Ensures payroll entries are correctly associated with users and departments for reporting.
6. **Integration with Multi-Company and Intercompany Operations**
    - Automated Role Segmentation: User permissions adapt automatically to the company context.
    - Intercompany Data Control: Ensures that imported/exported data respects company boundaries and access rules.
7. **Integration with External Tools**
    - BI and Reporting Systems: Export structured data to external analytics platforms.
    - External Databases or Legacy Systems: Import legacy data while preserving security and access configurations.
    - Third-Party Applications: Integrates with external HR, ERP, or compliance tools for seamless data flow.
8. **Audit and Compliance Integrations**
    - Logs all administrative actions for internal review and regulatory compliance.
    - Exports audit reports for external auditors or internal control teams.
    - Tracks changes to permissions, user roles, and imported/exported datasets.

4.2 External System Integrations for Administrative Management and Data Import/Export

While Odoo provides a comprehensive administrative and data management suite, many organizations need to integrate their administrative systems with external platforms such as HR

systems, payroll providers, compliance tools, legacy ERP systems, or BI platforms. Odoo supports a range of external integrations—both native and via APIs or third-party connectors—to ensure secure data exchange, compliance, and operational efficiency.

1. **HR and Payroll Systems**
    - Employee Data Sync: Import user accounts, department assignments, and role details from external HR platforms (e.g., ADP, BambooHR, Gusto) to create and manage Odoo users automatically.
    - Payroll Integration: Import payroll summaries to generate accounting and administrative records, avoiding manual entry.
    - Compliance Support: Ensures user roles and access rights reflect organizational hierarchies and legal obligations.
2. **External Access Control and SSO Systems**
    - Single Sign-On (SSO) Integration: Connect with LDAP, Active Directory, or OAuth providers to authenticate users centrally.
    - Role Mapping: Map external groups or roles to Odoo groups for consistent access management.
    - Real-Time Sync: Changes in external identity systems propagate to Odoo automatically.
3. **Legacy ERP or Custom Systems**
    - API-Driven Integration: Use Odoo's RESTful API or XML-RPC interface to import/export administrative and master data.
    - Examples: Sync users, groups, permissions, or departmental hierarchies; import legacy datasets for onboarding or migration.
    - Middleware Solutions: ETL tools like Zapier, Make (Integromat), or custom scripts bridge Odoo with any external system.
4. **Document Management and E-Signature Tools**
    - Integrate with DocuSign, Adobe Sign, or PandaDoc to securely manage administrative documents.
    - Automate workflows for approvals, role assignments, or data validation.
    - Ensures auditable records for compliance and governance.
5. **Audit and Compliance Platforms**
    - Export logs and administrative data in standardized formats (e.g., CSV, JSON, XBRL) for internal or external audits.
    - Connect with compliance monitoring platforms to track changes in access rights and user activity.

- Provides transparency and accountability for administrative operations.

6. **Business intelligence and Reporting Systems**

   - Export structured administrative data for analysis in external BI or reporting tools.
   - Supports dashboards that track user activity, import/export volumes, and permission changes.
   - Enables proactive monitoring of data governance and operational efficiency.

Chapter 5

Core Concepts and Key Digital Documents

5.1 Key Concepts: Administrative Management, Access Rights, and Data Import/Export

To use Odoo efficiently for administration, access control, and bulk data management, it's essential to understand its foundational concepts. These "building blocks" form the backbone of your administrative operations, ensure security and compliance, and streamline data handling. This section explains the core pillars:

1. **User Roles and Access Rights (The Security Blueprint)**

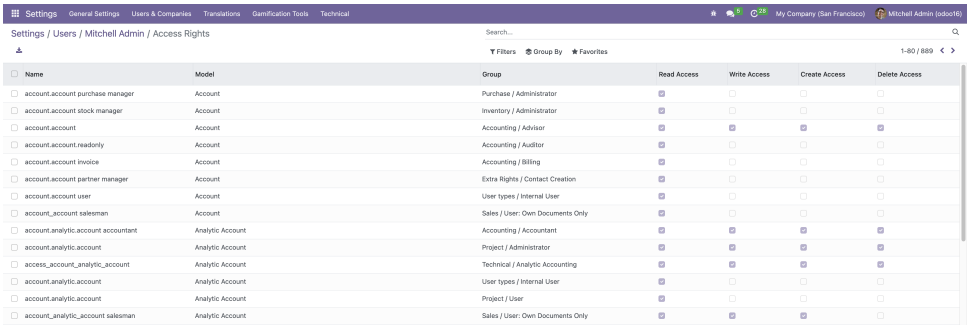

Figure 5.1: User Roles and Access Rights

Odoo's access control system defines who can do what within the platform. Proper configuration ensures that users only access the data they are authorized to see or modify.

- Role Hierarchy: Users are assigned to groups with predefined permissions (e.g., Accountant, Finance Manager, Administrator, HR Officer).
- Record Rules: Control access at a record level, ensuring sensitive data is protected.
- Multi-Company Context: Users see only records relevant to their assigned companies.
- Best Practice: Define roles conservatively—grant only the permissions necessary for each user's job function.

2. **Groups and Permissions (Compliance by Design)**

   Groups aggregate users with similar roles and control access to Odoo modules and specific actions.

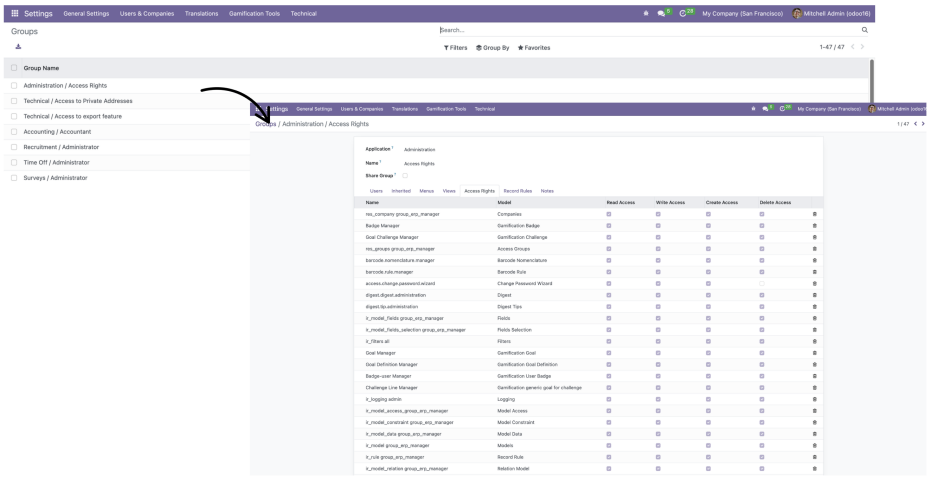

Figure 5.2: Groups and Permissions

- Predefined Groups: Odoo ships with default groups like “Accountant,” “Manager,” and “Portal User.”
- Custom Groups: Administrators can create groups for special projects or departments with tailored access rules.
- Module-Level Access: Grant or restrict module usage (e.g., Sales, HR, Inventory) per group.
- Action-Level Permissions: Define what users can create, read, update, or delete within each module.

3. **Import/Export Framework (Data Management Engine)**

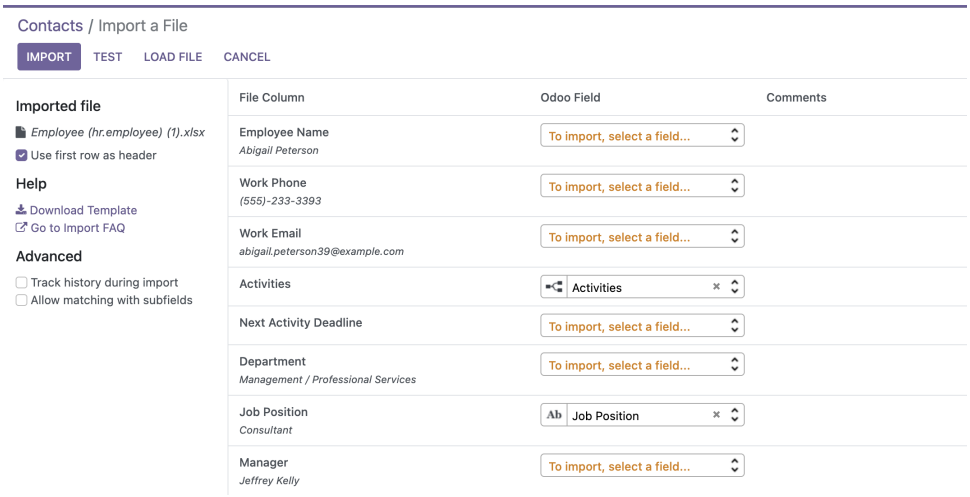

Figure 5.3: Data Import/Export Architecture

Odoo provides robust tools to import bulk data, export records, and integrate with external systems securely.

- Import Templates: Preconfigured CSV/XLSX templates for importing users, roles,

employees, or departmental hierarchies.

- Data Validation: Automatically checks for duplicates, missing fields, or permission violations.
- Export Options: Extract user activity logs, role assignments, and audit trails in standard formats for reporting or BI tools.
- API Access: REST and XML-RPC APIs allow secure integration with external HR, ERP, or compliance systems.
- Bulk Operations: Supports mass updates, role assignments, and data migration without manual entry.

4. **Audit Trail and Compliance (Transparency at a Glance)** All administrative actions are logged to ensure accountability and meet regulatory or internal governance requirements.

   - Track Changes: Logs when roles, permissions, or user records are added, modified, or removed.
   - Exportable Reports: Audit logs can be exported for internal reviews or external audits.
   - Real-Time Monitoring: Dashboards track data import/export activity and permission changes.
   - Compliance Enforcement: Ensures access rights, imports, and exports comply with organizational policies and legal requirements.

5.2 Important Documents in the Workflow:

1. **User Access Request Form**

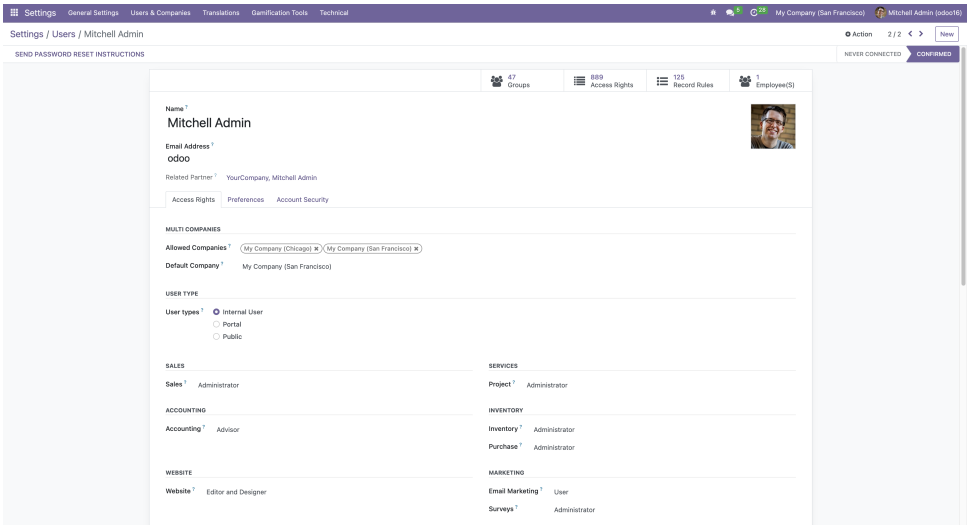

Figure 5.4: User Access Request Form

- Purpose: A formal request submitted by employees or departments to gain access to specific Odoo modules or functionalities.
- Key Elements: Request ID, employee details, requested access groups, justification, manager approval, and date of request.
- Workflow: Submitted by the requester, reviewed by the manager, assigned to the administrator, approved or rejected, and applied within the Odoo access rights configuration.

2. **User Creation / Modification Record**

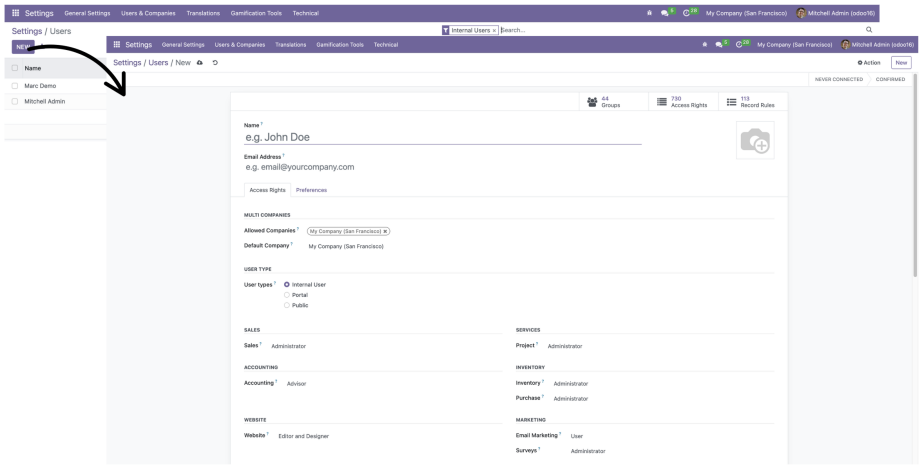

Figure 5.5: User Creation or Modification Record

- Purpose: A document that tracks the creation of a new user or updates made to an existing user account.
- Key Elements: User name, email, assigned groups, company access, modification history, and activation status.
- Workflow: Created by administrators when onboarding new staff, updating roles, or adjusting permissions; logged for audit and compliance.

3. **Access Rights Matrix**

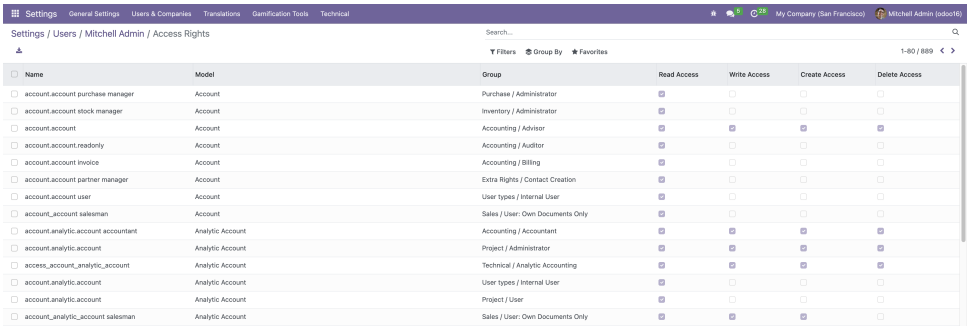

Figure 5.6: Access Rights Matrix

- Purpose: A structured document outlining module-level and record-level permissions for each user group.
- Key Elements: List of groups, CRUD permissions (Create/Read/Update/Delete), module access, record rules, and company-specific restrictions.
- Workflow: Reviewed during system audits, security checks, and onboarding; updated when new modules or roles are introduced.

4. **Data Import File (CSV/XLSX Template)**

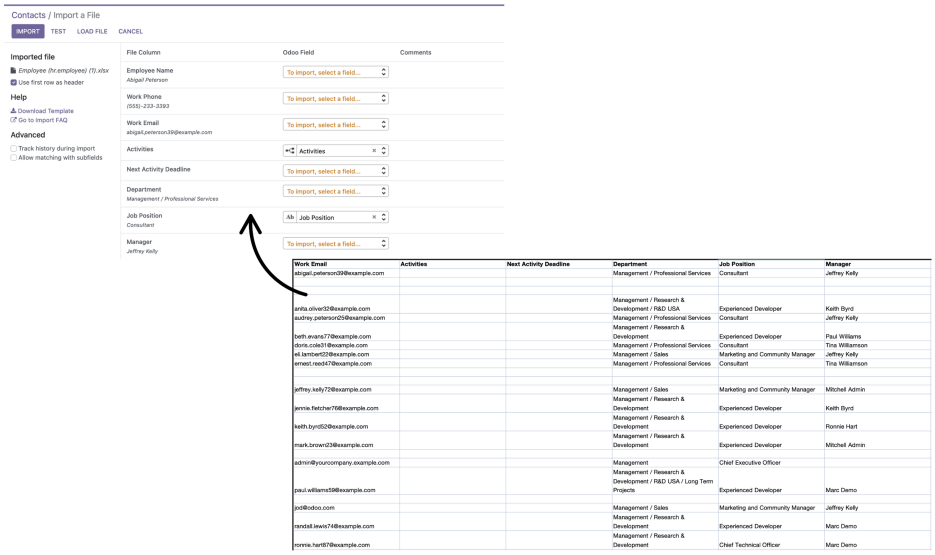

Figure 5.7: Import Template

- Purpose: A spreadsheet used for bulk importing data such as users, departments, employees, or access groups into Odoo.
- Key Elements: Field column headers, external IDs, relational fields, data types, and reference values.
- Workflow: Prepared using Odoo export templates, filled with clean data, uploaded through the Import tool, validated, and applied to the system.

5. **Data Export Report**

- Purpose: A structured dataset extracted from Odoo for reporting, analysis, migration, or integration with external applications.
- Key Elements: Selected fields, filters applied, file format (CSV/XLSX), export timestamp, and user who exported the data.
- Workflow: Generated using the Export tool, shared with departments, used for BI reporting, or provided during audits.

Name	duct Categ	roduct Typ	ense Account
Adopter (T)	All / Office	Storable Pr	6230 – Office Supplies Expense
Ball Pen (B	All / Office	Storable Pr	6230 – Office Supplies Expense
Calculator	All / Office	Storable Pr	6230 – Office Supplies Expense
Laptop	All	Storable Pr	1500 – Property, Plant, and Equipment
Soap	All	Consumab	6200 – Other Expense
Rice	All / Kitcher	Storable Pr	6210 – Kitchen Expense
Chair	All	Storable Pr	1540 – Furniture and Fixtures
Colin	All	Consumab	6200 – Other Expense
AC	All	Storable Pr	6280 – Professional and Administrative Expenses
TV	All	Storable Pr	6280 – Professional and Administrative Expenses

Figure 5.8: Data Export

6. **Audit Log / Activity Record**

- Purpose: A chronological record of administrative activities such as user access changes, data imports/exports, and permission modifications.
- Key Elements: Action type, user performing the action, timestamp, before/after values, affected module, and company/environment.
- Workflow: Automatically generated by Odoo; reviewed during audits, compliance checks, troubleshooting, or when investigating data inconsistencies.

Part III

The Operational View: Workflows and Processes

Chapter 6

The Administrative Workflow: A Deep Dive

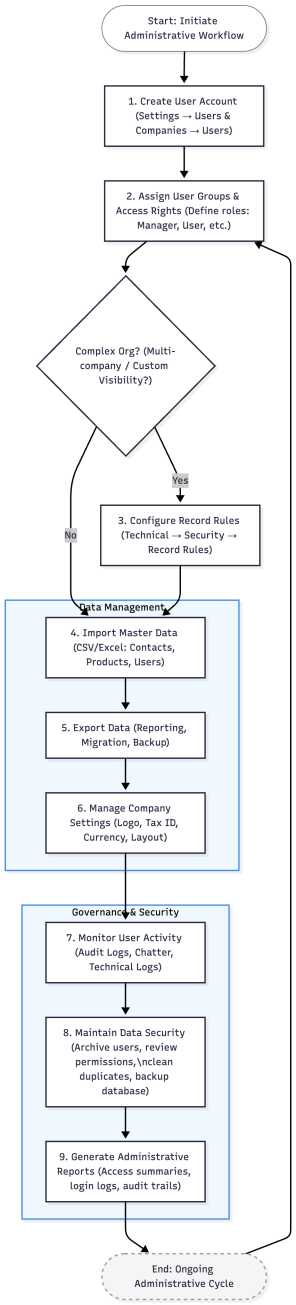

Figure 6.1: Administrative Workflow

This workflow demonstrates the end-to-end process of managing users, permissions, and organizational data using Odoo's administrative tools.

1. Create a User Account

   Purpose: Add a new system user with appropriate access so they can work within Odoo.

   Steps:

   - Navigate to Settings → Users & Companies → Users.
   - Click Create.
   - Enter:
     - Name and Email
     - Optional: Phone, Job Position, Company
   - Under Access Rights, choose the applications and permission levels (e.g., Administrator, Manager, User).
   - Under Preferences, configure:
     - Language
     - Timezone
     - Notification settings
   - Save the record. The user receives an invitation email to set their password.

   Tip: Users can also be created automatically when adding employees in the Employees app.

2. Configure User Groups

   User Groups define permission sets (technical and functional) shared among multiple users.

   Steps:

   - Go to Settings → Users & Companies → Groups.
   - Select a group to edit (e.g., Sales Manager, Accountant, Inventory User).
   - Review the assigned:
     - Menu access
     - Model access (read, write, create, delete)
     - Record rules
   - Add or remove users from the group.

   Tip: A user can belong to multiple groups, and permissions are combined.

3. Manage Record Rules

   Purpose: Restrict what specific records a user can access (e.g., "User sees only their own records"). Record Rules apply at the database level and enforce data security.

   Steps:

- Enable Developer Mode.
- Navigate to Settings → Technical → Security → Record Rules.
- Choose or create a rule:
  - Select the model (e.g., res.partner, sale.order)
  - Add domain filters (e.g., ['|', ('company_id','=',user.company_id.id)])
  - Assign it to one or more security groups
  - Set the permissions (read, write, create, delete)
- Save to apply the rule.

Examples:

- Sales users only see their own customers.
- HR Officers can view all employee data, but regular users cannot.

4. Import Master Data (Users, Contacts, Products, etc.)

   Purpose: Add or update large amounts of data efficiently.

   Steps:

   - Go to any list view (e.g., Contacts, Products, Users).
   - Click Import.
   - Upload a CSV or Excel file.
   - Use Test Import to validate:
     - Column mapping
     - Data types
     - Required fields
     - External IDs (for updating existing data)
   - Fix any warnings or errors.
   - Click Import to finalize.

   Tip: Export a sample template with fields you want to fill in.

5. Export Data for Reporting or Migration

   Purpose: Retrieve data for external systems, audits, or backups.

   Steps:

   - Go to a list view.
   - Select the records (optional).
   - Click Action → Export.
   - Choose:
     - Export format: CSV or Excel

    - Export type:
        * Import-Compatible Export
        * Export All Data
- Select fields to include.
- Export the file.

Tip: Use Export-Compatible when planning to re-import later.

6. Manage Company Settings

   Purpose: Configure organizational identity and system-wide defaults.

   Steps:

   - Go to Settings → Users & Companies → Companies.
   - Edit company details:
       - Address, Contact Info
       - Logo
       - Currency, Tax ID
       - Document layout settings
   - Configure multi-company if applicable.

   Tip: Permissions and record visibility depend heavily on company configuration in multi-company setups.

7. Monitor User Activity

   Purpose: Track performance, identify errors, and ensure system security.

   Tools:

   - Audit Log (Enterprise): Tracks user operations.
   - Logs under Settings → Technical → Logs.
   - Discuss App: Shows message and notification history.
   - Chatter on Records: Shows who modified which record.

8. Maintain Data Security and Cleanup

   Purpose: Ensure clean, accurate, and secure records.

   Actions:

   - Archive inactive users instead of deleting.
   - Regularly review Access Rights and Groups.
   - Clean duplicate data using the “Duplicates” tool (if installed).
   - Backup the database via:
       - Odoo.sh backups

- Manual backups from the database manager

9. Generate Administrative Reports

   Common administrative reports include:

   - User Access Summary
   - Login Activity Reports
   - Audit Logs (Enterprise)
   - Data Import/Export Logs
   - Company Configuration Summaries

   Access via Settings → Technical or via imported/exported files.

6.1 From Anonymous Visitor to Authorized System User: An Administrative Sequence Diagram

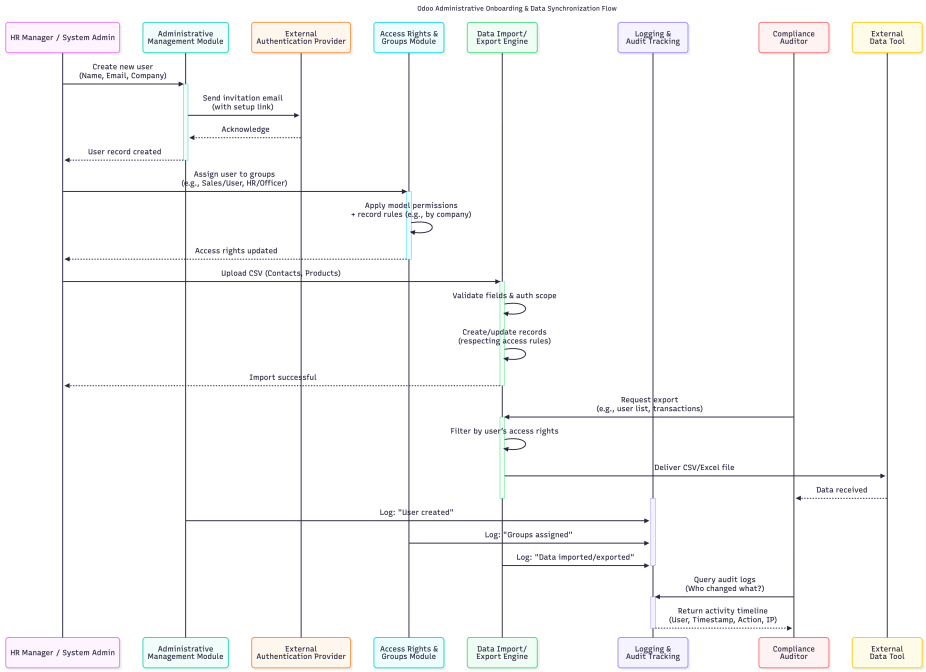

Figure 6.2: Administrative User Onboarding and Data Synchronization Sequence

Overview of key administrative processes:

- **User Account Creation & Invitation**
- An **HR Manager** or **System Administrator** initiates user creation via the Odoo interface.
- The **Administrative Management Module** creates a user record and sends an automated email invitation.

- The new user accesses the system via a secure link, sets a password, and is authenticated (optionally via an **External Authentication Provider** such as LDAP or OAuth).
- **Assignment of Access Rights and Groups**
- The **System Administrator** assigns the user to one or more **Security Groups** (e.g., Sales / User, HR / Officer).
- The **Access Rights & Groups Module** applies model-level permissions (read/write/create/delete) and menu visibility.
- Record-level rules are enforced based on group membership (e.g., "Sales users see only their own leads").
- **Bulk Data Import (e.g., Contacts, Products)**
- An **Administrator** uploads a CSV file via the **Data Import/Export Engine**.
- The system validates field mapping, data types, and required constraints.
- Valid records are created or updated in the respective modules (e.g., Contacts in CRM, Products in Inventory), respecting user access rights.
- **Data Export for Audit or Migration**
- A **Compliance Auditor** or **Department Manager** requests an export of user or transactional data.
- The **Data Import/Export Engine** generates a structured CSV/Excel file containing only records the user is authorized to view.
- The file is downloaded or sent to an **External Data Tool** for analysis.
- **Multi-Company Access Restriction**
- In a multi-company setup, the **User Management Module** links the user to one or more companies.
- The **Record Rules Engine** automatically filters data by company (e.g., a user in "Company A" cannot see invoices from "Company B").
- This restriction is applied transparently across all modules (Sales, HR, Accounting).
- **Activity Logging and Audit Trail**
- All administrative actions (user creation, permission changes, data imports) are logged by the **Logging & Audit Tracking Module**.
- A **Compliance Auditor** queries the audit log to verify who changed what and when.
- Logs include user ID, timestamp, affected records, and IP address (in Odoo Enterprise).

6.2 BPMN Diagram: The End-to-End Administrative Governance Process

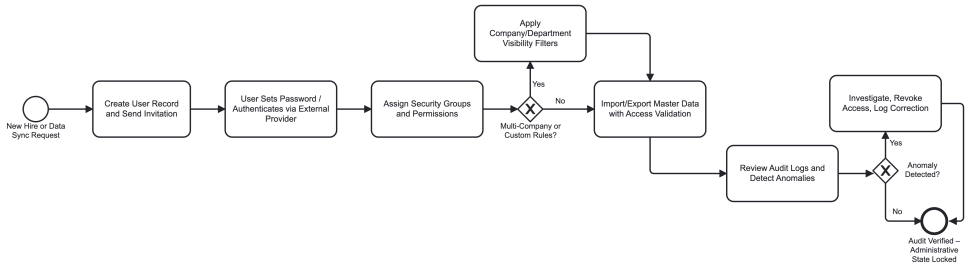

Figure 6.3: Administrative User and Data Lifecycle in Odoo

The Odoo Administrative Management process is structured into four interconnected governance phases: **User Provisioning**, **Access Control**, **Data Synchronization**, and **Compliance & Audit**. This end-to-end workflow ensures secure onboarding, least-privilege access, accurate master data, and regulatory readiness.

In **User Provisioning**, the process begins when HR or a Department Manager requests a new system user (e.g., for a new hire). A draft user record is created in Odoo, triggering an automated invitation email. The user sets their password—optionally authenticated via an external identity provider (e.g., LDAP/SAML). Upon first login, their account is activated and linked to one or more companies in multi-company setups.

Next, in **Access Control**, the System Administrator assigns the user to appropriate security groups (e.g., "Sales / User", "HR / Officer"). These groups enforce model-level permissions (read/write/create/delete) and menu visibility. Additionally, record rules are applied to restrict data access—for example, sales representatives only see their own customers, or employees are limited to their department's records. Any changes to group membership are logged in real time.

The **Data Synchronization** phase handles bulk operations. Administrators regularly import master data (e.g., contacts, products, or employee records) via CSV or Excel files. The Data Import/Export Engine validates field mappings, checks data integrity, and ensures new records comply with access rules. Conversely, data exports are generated for reporting, migration, or third-party integration—always filtered to include only records the requester is authorized to view.

Finally, in **Compliance & Audit**, the system enforces ongoing governance. Periodically—or upon request—a Compliance Auditor reviews the audit log, which captures all administrative actions: user creations, permission changes, data imports/exports, and login attempts. If anomalies are detected (e.g., a user granted excessive privileges), the issue is investigated, access is revoked or adjusted, and corrective entries are logged. Once verified, the audit trail is archived, and the administrative state is considered compliant and locked for the review period.

This closed-loop administrative process ensures that every user, permission, and data record is

traceable, secure, and aligned with organizational policies—forming the foundation of trustworthy ERP operations in Odoo.

6.3 Step-by-Step Breakdown of the Administrative Governance Journey

"How we provision users, enforce access controls, synchronize data, and ensure compliance."

This journey reflects the end-to-end administrative lifecycle in Odoo, structured around four core capabilities: **User Provisioning**, **Access Rights Management**, **Data Import/Export**, and **Audit & Compliance**. Every step ensures security, accuracy, and regulatory readiness.

User Provisioning – From Request to Active Account

- **User Request Initiated (Start Event)**
  → Triggered by HR or a Department Manager (e.g., for a new hire, contractor, or system access request).
- **Create Draft User Record**
  → Navigate to `Settings → Users & Companies → Users → Create`.
  → Enter name, email, company, and job position. Account is inactive until invitation is accepted.
- **Send Invitation Email**
  → Odoo sends a secure, time-limited setup link. No password is stored yet.
- **User Activates Account (Message Event)**
  → User clicks link, sets password, and logs in for the first time.
  → Optional: Authentication delegated to **External Provider** (LDAP, OAuth, SAML).
- **Account Activated (End of Provisioning)**
  → User exists in system but has *no permissions* until groups are assigned.

Access Rights Management – Enforcing Least Privilege

- **Assign Security Groups**
  → Admin assigns user to one or more groups (e.g., *Sales / User*, *Inventory / Manager*).
  → Groups control **menu access**, **model permissions** (read/write/create/delete), and **record rules**.
- **Multi-Company Environment? (Decision Gateway)**
- **Yes** → Apply company-based **record rules** (e.g., "Only see customers from your company").

- **No** → Standard group permissions apply across all data.
- **Validate Access Scope**
  → Admin logs in as the user (via `Impersonate`) or reviews visible records to confirm least-privilege compliance.
- **Access Configuration Complete (Milestone)**
  → User can now perform authorized tasks. All permission changes are logged.

Data Import/Export – Managing Master Data at Scale

- **Initiate Bulk Data Operation (Start Event)**
  → Admin prepares CSV/Excel file (e.g., contacts, products, employee records).
- **Import Master Data**
  → Go to list view (e.g., Contacts), click `Import`, and upload file.
  → Map columns using Odoo's field-matching interface.
- **Validate Data Integrity & Permissions**
  → Odoo checks:
- Required fields and data formats
- Duplicate records (if deduplication enabled)
- Whether the importing user has `create/write` rights on target model
- **Import Successful? (Decision Gateway)**
- **Yes** → Records created/updated. Success log generated.
- **No** → Errors shown (e.g., invalid email, missing required field). Admin corrects file and retries.
- **Export Filtered Data**
  → Select records (or use filters), click `Action → Export`.
  → Choose fields and format (CSV/Excel).
  → Output is automatically filtered: **user only sees data they have access to**.

Audit & Compliance – Ensuring Governance and Traceability

- **Audit Cycle Initiated (Timer or Manual Event)**
  → Triggered monthly, quarterly, or on-demand by Compliance Officer.
- **Review Audit Logs**
  → Access `Settings → Technical → Logs → Audit Logs` (Odoo Enterprise) or system logs.
  → Logs capture: user creations, group changes, data imports/exports, login attempts, and configuration updates.

- **Anomaly Detected? (Decision Gateway)**
- **Yes** → Investigate (e.g., user granted Admin rights unexpectedly). Revoke access, log corrective action, notify stakeholders.
- **No** → Proceed to archival.
- **Archive Verified Audit Trail**
  → Export logs to secure external storage (e.g., encrypted backup, compliance repository).
- **Administrative State Locked (End Event)**
  → Period marked as compliant. Critical configurations (users, groups, company settings) are considered frozen for audit purposes.
  → In Odoo: Use `Settings → Users & Companies → Companies` to review and lock key settings.

This closed-loop administrative journey ensures that every user, permission, and data record in Odoo is **secure**, **traceable**, and **compliant**—laying the foundation for trustworthy ERP operations.

Chapter 7

Daily Operations and Integrated Processes

7.1 The Daily Administrative Governance Process

To maintain a secure, compliant, and efficient Odoo environment, it's essential to perform routine administrative tasks daily. This section outlines key daily activities for your System Administrator,HR Manager, or Compliance Officer using Odoo's Administrative Management, Access Rights, and Data Import/Export capabilities.

Recommended: Assign these tasks to a responsible team member and complete them before end-of-day to ensure data integrity and access control.

1. **Review and Activate New User Requests**
2. Go to `Settings → Users & Companies → Users`
   (a) Identify draft or invited users (e.g., new hires, contractors).
   (b) Verify company assignment and contact details.
   (c) Resend invitation if needed, or archive stale requests.
   (d) *Tip: Enable "Employee" creation in HR app—users are auto-created when employees are added.*
3. **Audit User Access and Group Assignments**
4. Review recently modified users under `Settings → Users & Companies → Users → Filter: "Last Updated Today"`.
   (a) Confirm that security groups align with job roles (e.g., "Sales / User", "HR / Officer").
   (b) Remove unnecessary permissions or expired access (e.g., for departing employees).
   (c) *Best Practice: Apply "least privilege" – users should only access what they need.*
5. **Monitor and Validate Data Imports**
6. Check `Settings → Technical → Imports` (or recent activity logs) for failed or pending imports.

7. Validate recently imported master data (e.g., contacts, products, employees):
   - Ensure records appear in correct company (in multi-company setups)
   - Confirm no duplicates were created
   - Verify required fields are populated
   - Clean or reprocess any failed imports using corrected CSV files.
8. **Process Data Export Requests**
9. Respond to requests from managers or auditors for data exports (e.g., user lists, contact exports).
   (a) Navigate to relevant list view (e.g., `Contacts`, `Users`), apply filters, and click `Action → Export`.
   (b) Ensure exports are **filtered by requester's access rights**—Odoo automatically enforces this.
   (c) Deliver files securely (e.g., encrypted email, internal portal).
10. **Review Audit and Login Activity**
11. In Odoo Enterprise: Go to `Settings → Technical → Logs → Audit Logs`.
12. Check for:
    - Unusual login attempts (e.g., from new locations)
    - Bulk permission changes
    - Unauthorized data exports
    - In Community Edition: Review server logs or use third-party audit modules.
    - Investigate anomalies immediately and escalate if needed.
13. **Maintain Company and System Configuration**
14. Go to `Settings → Users & Companies → Companies`
15. Verify:
    - Company details (address, tax ID, currency) are up to date
    - Document templates (invoices, quotes) reflect current branding
    - Multi-company rules are correctly configured
    - Ensure external integrations (e.g., LDAP, SAML) are operational.
16. **Perform Backup and System Health Check (Recommended)**
17. Confirm that:
    - Automated database backups ran successfully (via Odoo.sh or on-premise scripts)
    - User authentication (local or external) is functioning

- Email delivery for system notifications (e.g., invitations) is working
- Archive or deactivate inactive users instead of deleting—preserves data integrity.

By performing these tasks daily, your organization ensures that user access remains secure, master data stays accurate, and compliance requirements are continuously met—forming the foundation of a trustworthy Odoo ERP environment.

7.2 Operational Workflow for Administrative Governance

This workflow outlines the standard operating procedures for managing user identities, access rights, master data, and compliance in Odoo. It ensures security, data integrity, and regulatory readiness across User Management, Access Control, Data Synchronization, and Audit Logging.

Scope: Applies to all Odoo deployments—whether using Sales, HR, Accounting, or custom modules—since administrative governance is foundational to every instance.

1. **User & Company Setup**
   (a) **Create New User**
   (b) Go to `Settings → Users & Companies → Users → Create`
   (c) Enter:
      - Full name, work email, phone (optional)
      - Associated **Company** (critical in multi-company setups)
      - Language, timezone, and notification preferences
      - *Note: No permissions are granted yet—groups are assigned separately.*
      - Save → Odoo sends an automated invitation email with a setup link.
   (d) **Configure Company Settings**
   (e) Go to `Settings → Users & Companies → Companies`
   (f) Edit or create company records with:
      - Legal name, address, tax ID
      - Logo and document layout (for reports, invoices)
      - Default currency and fiscal localization
      - In multi-company mode, ensure inter-company rules are defined.

   Tip: Users can be auto-created when adding employees in the `Employees` app.

2. **Access Rights Management**
   (a) **Assign Security Groups**
   (b) Open the user record → Go to `Access Rights` tab.
   (c) Assign one or more groups (e.g., *Sales / User*, *Inventory / Manager*).

(d) Groups control:

- Menu visibility
- Model-level permissions (read/write/create/delete)
- Record rules (e.g., "Only see own leads")

(e) **Review Custom Record Rules (Advanced)**

(f) Enable `Developer Mode`

(g) Go to `Settings → Technical → Security → Record Rules`

(h) Verify rules for sensitive models (e.g., `res.users`, `hr.employee`)

(i) Example: A rule like `[('company_id', '=', user.company_id.id)]` enforces company isolation.

Best Practice: Audit group assignments quarterly to remove unnecessary access.

3. **Data Import Operations**

(a) **Prepare and Import Master Data**

(b) From any list view (e.g., `Contacts`, `Products`), click `Import`.

(c) Download template to ensure correct field mapping.

(d) Upload CSV or Excel file with:

- External IDs (for updates)
- Required fields (e.g., email for contacts)
- Company assignment (in multi-company setups)

(e) **Validate and Troubleshoot**

(f) Use `Test Import` to preview results.

(g) Fix errors (e.g., invalid emails, missing required fields).

(h) Confirm import only after validation succeeds.

(i) *Note: Imported records respect the importer's access rights—restricted users cannot create privileged data.*

4. **Data Export Operations**

(a) **Export Filtered Data**

(b) Apply filters or select specific records in a list view.

(c) Click `Action → Export`.

(d) Choose fields and format (CSV or Excel).

(e) **Critical: Odoo automatically filters the export to include only records the user is authorized to view.**

(f) **Use Cases**

(g) HR exports employee lists for payroll

(h) Auditors request user access summaries

(i) Managers extract customer contact lists for campaigns

5. **Authentication & External Integration**

   (a) **Configure External Authentication**

   (b) Go to `Settings → Activate Developer Mode`

   (c) Navigate to `Settings → Technical → Authentication → OAuth Providers` (or LDAP)

   (d) Connect to identity providers (e.g., Google Workspace, Azure AD, LDAP)

   (e) Test login flow to ensure SSO works.

   (f) **Verify User Login Activity**

   (g) Check last login timestamp on user records.

   (h) Archive or deactivate inactive users (>90 days) to reduce risk.

6. **Audit, Logging & Compliance**

   (a) **Review Audit Logs (Odoo Enterprise)**

   (b) Go to `Settings → Technical → Logs → Audit Logs`

   (c) Filter by date, user, or model (e.g., `res.users`, `ir.attachment`)

   (d) Logs include: user, action, timestamp, IP address, and field changes.

   (e) **Compliance Controls**

   (f) Restrict access to sensitive menus via group permissions.

   (g) Enable two-factor authentication (2FA) for admins (via Odoo Enterprise or third-party modules).

   (h) Archive (don't delete) users to preserve historical data integrity.

   (i) **Backup Strategy**

   (j) Ensure daily automated backups (via Odoo.sh, server cron, or cloud provider).

   (k) Test restore procedures quarterly.

7. **Periodic Administrative Review**

8. **Weekly**: Review new user requests, failed imports, login anomalies.

9. **Monthly**: Audit group memberships, company settings, and export logs.

10. **Quarterly**: Validate external auth integrations and backup integrity.

11. **After Employee Offboarding**: Immediately revoke access and archive user.

7.3 Administrative Integration

Odoo's Administrative Management framework acts as the **governance backbone** of your system, integrating natively with all Odoo modules to enforce consistent user access, secure data handling, and seamless master data synchronization. This section outlines key administrative integrations that enhance security, compliance, and operational efficiency.

Note: All integrations described below are native (no third-party connectors required) and active by default when using Odoo's standard apps.

1. **Integration with All Modules via Access Rights**

   How It Works:

   (a) User permissions are centrally managed in `Settings → Users & Companies → Groups`.

   (b) Each module (Sales, HR, Inventory, etc.) defines its own security groups (e.g., *Sales / User*, *HR / Officer*).

   (c) When a user is assigned to a group, they automatically gain:

      i. Access to relevant menus

      ii. Permissions to read/write/create/delete records

      iii. Visibility rules (e.g., "only see own customers")

   Benefits:

   (a) Single source of truth for user permissions

   (b) No need to configure access separately in each app

   (c) Real-time enforcement of least-privilege principles

   Where It Applies:

   (a) A Sales user cannot access HR employee records unless granted explicit HR group access.

   (b) An Inventory user sees only products and locations permitted by their group's record rules.

2. **Integration with HR (Employees App)**

   How It Works:

   (a) When an employee is created in `Employees → Create`, Odoo can automatically:

      i. Create a corresponding **user account**

      ii. Link the user to a company and job position

      iii. Assign default security groups based on department or role

   (b) User deactivation is synchronized: archiving an employee can auto-deactivate their login.

Benefits:

(a) Eliminates duplicate HR and IT workflows

(b) Ensures immediate access provisioning for new hires

(c) Reduces risk of orphaned accounts during offboarding

Configuration:

(a) Enable in `Settings → Users & Companies → Check "Employee" field on user form`

(b) Or enable "Create User" checkbox when creating an employee

3. **Integration with Data Import/Export Across Modules**

How It Works:

(a) The **Data Import/Export Engine** is available in every list view (Contacts, Products, Users, etc.).

(b) When importing data, Odoo:

i. Validates field mappings using the target module's data model

ii. Enforces the **importer's access rights**—users cannot create records they don't have permission to view

iii. Uses External IDs to update existing records reliably

(c) Exports are automatically filtered: users only export data they are authorized to see.

Benefits:

(a) Consistent data governance across all modules

(b) Secure bulk operations without exposing sensitive data

(c) No need for module-specific import tools

Example:

(a) An HR manager imports 50 new employees → user accounts are created only if they have `User` creation rights.

(b) A Sales manager exports customers → only sees customers assigned to their team or company.

4. **Integration with External Authentication Providers**

How It Works:

(a) Odoo supports native integration with:

i. LDAP/Active Directory

ii. OAuth 2.0 (Google, Azure AD, GitHub)

iii. SAML (via Odoo Enterprise)

(b) User authentication is delegated externally, but **permissions remain managed in Odoo**.

(c) User provisioning can be just-in-time (JIT): first login creates a minimal user record, which admins can later enrich.

Benefits:

(a) Centralized identity management (SSO)

(b) Eliminates password fatigue and improves security

(c) Complies with enterprise identity policies

Configuration:

(a) `Settings → Activate Developer Mode`

(b) `Settings → Technical → Authentication → [LDAP/OAuth/SAML]`

5. **Integration with Audit Logging (Odoo Enterprise)**

How It Works:

(a) The **Audit Log** module tracks changes across all apps:

i. User creations and group assignments

ii. Data imports and exports

iii. Record modifications (e.g., contact email changed)

iv. Login attempts and session activity

(b) Logs include: user, timestamp, IP address, and field values before/after changes.

Benefits:

(a) End-to-end traceability for compliance (SOX, GDPR, ISO 27001)

(b) Detects unauthorized access or data tampering

(c) Simplifies forensic investigations

Access:

(a) `Settings → Technical → Logs → Audit Logs` (Odoo Enterprise only)

Part IV

Configuration, Data, and Analytics

Chapter 8

Configuration and Underlying Business Logic

8.1 Documenting Administrative Configuration Settings

Proper configuration of Odoo's administrative framework ensures secure user access, consistent data governance, and compliance with internal policies and external regulations. This section documents all key administrative settings that must be reviewed and configured before going live—and periodically thereafter.

Access Path: Go to `Settings → Users & Companies`, `Settings → Activate Developer Mode → Technical`, or module-specific configuration menus.

1. **User Groups & Access Rights**

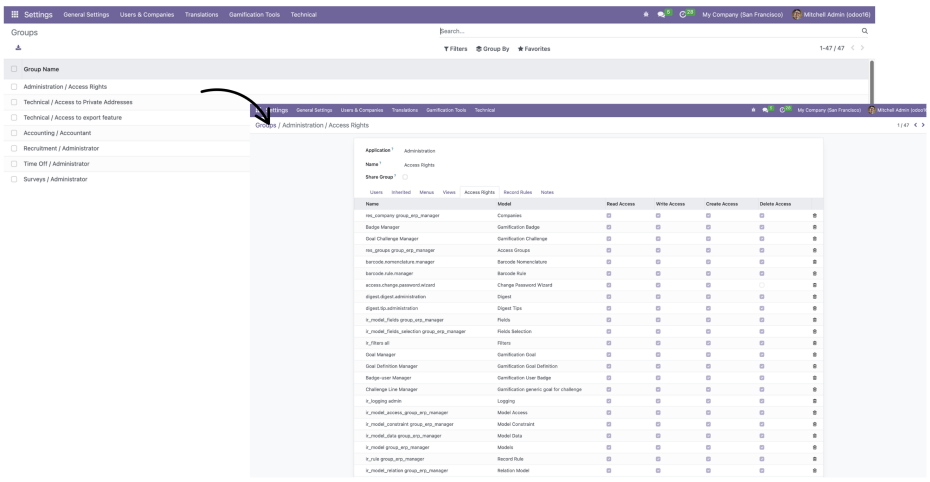

Figure 8.1: User Groups and Access Rights Setup

Purpose: Defines what users can see and do across all Odoo modules (Sales, HR, Accounting, etc.).

Configuration:

(a) Go to `Settings → Users & Companies → Groups`

(b) Review or create security groups (e.g., *Sales / Manager*, *HR / Officer*)

(c) For each group, configure:

i. Application access (which apps appear in menu)

ii. Model permissions (read/write/create/delete per data model)

iii. Record rules (e.g., "User sees only their own customers")

(d) Assign users to groups based on job roles—never grant direct record-level access.

Best Practice: Apply the principle of least privilege—users should only access what they need to perform their duties.

2. **Company Information & Multi-Company Setup**

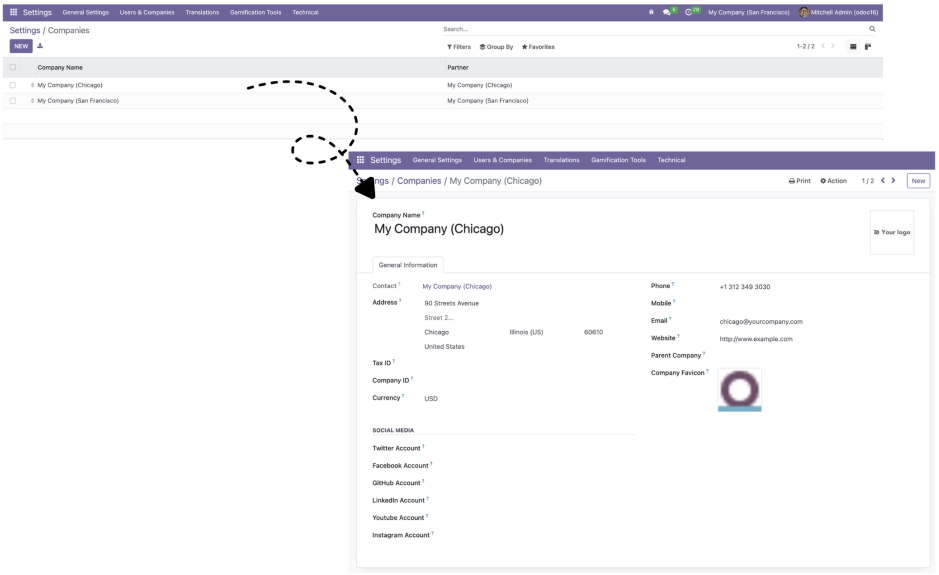

Figure 8.2: Company Information and Multi-Company Configuration

Purpose: Ensures data isolation and accurate user context in single or multi-company environments.

Configuration:

(a) Go to `Settings → Users & Companies → Companies`

(b) For each legal entity, configure:

i. Legal name, address, and contact details

ii. Logo (used in system emails and reports)

iii. Default currency and language

(c) In multi-company mode:

i. Assign users to one or more companies

ii. Enable `Settings → General Settings → Multi-Company`

iii. Verify record rules enforce company data separation

Critical for: Organizations with subsidiaries, branches, or separate legal entities.

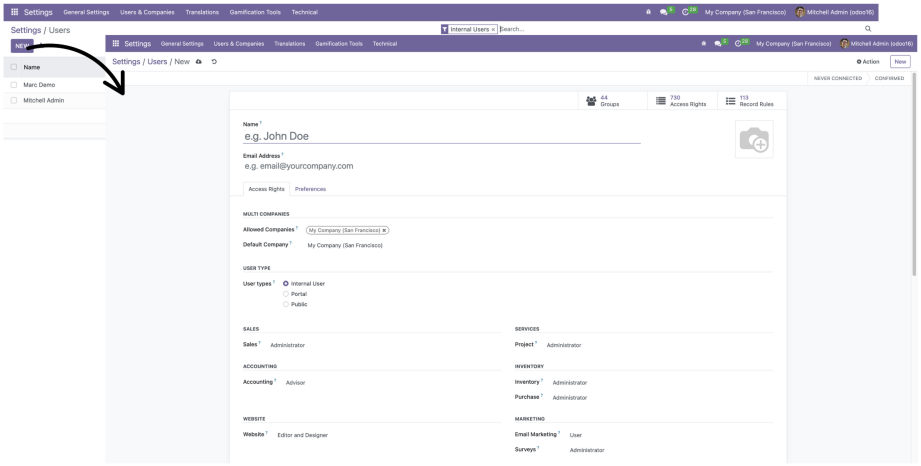

Figure 8.3: User Creation and Invitation Process

3. **User Creation and Onboarding Workflow**

   Purpose: Standardizes how new users are added, invited, and activated in the system.

   Configuration:

   (a) Go to `Settings → Users & Companies → Users → Create`

   (b) Ensure:

      i. Email is valid (used for invitation link)

      ii. Company is assigned (critical in multi-company setups)

      iii. Language and timezone are set

   (c) Save → Odoo sends an automated, secure setup email

   (d) Optional: Enable auto-user creation from the `Employees` app

   Note: Users have no permissions until assigned to a security group.

4. **Data Import/Export Engine Settings**

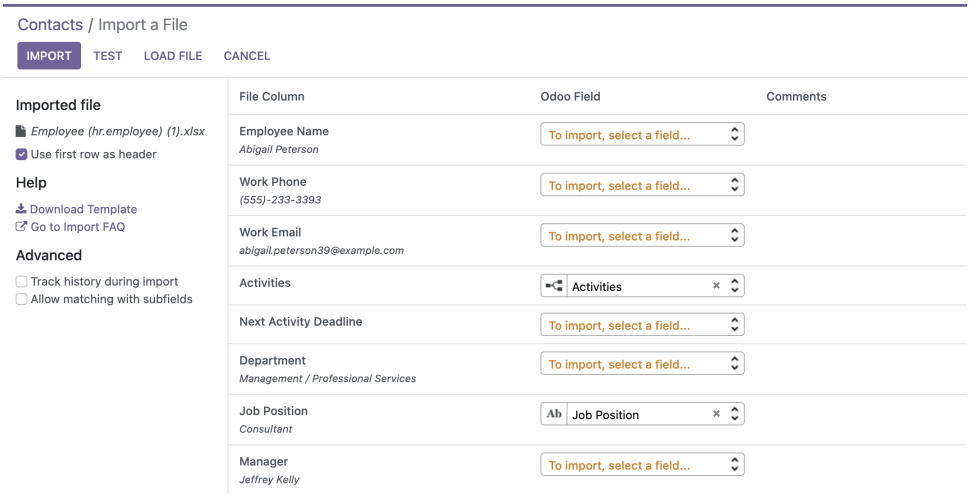

Figure 8.4: Data Import/Export Configuration

Purpose: Governs how bulk data is imported and exported across all modules.

Configuration:

(a) No global toggle—engine is available in every list view (Contacts, Users, Products, etc.)

(b) Ensure users have:

i. `Import` access (granted via group permissions)

ii. Write/create rights on target model

(c) For sensitive data, restrict export access via record rules or custom groups

(d) Use External IDs in imports to enable updates (not just creates)

Security Note: Exports are automatically filtered—users only see data they have access to.

5. **User Session and Security Policies**

Purpose: Controls session lifetime, password rules, and login security.

Configuration:

(a) Go to `Settings → Activate Developer Mode`

(b) Navigate to `Settings → Technical → Parameters → System Parameters`

(c) Key parameters:

i. `web.session.timeout`: Set session expiry (e.g., 3600 seconds)

ii. `auth.password_policy`: Enforce password complexity (Enterprise)

iii. `auth_totp`: Enable two-factor authentication (Enterprise)

(d) Regularly review and archive inactive users (>90 days)

Tip: Combine with external SSO for strongest security posture.

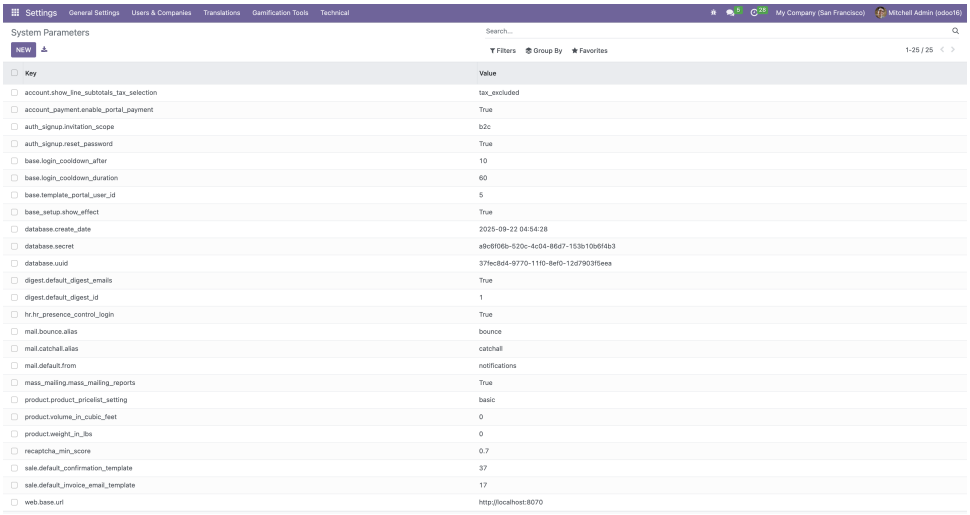

Figure 8.5: System Parameters for Security Policies

6. **Backup and Recovery Strategy**

   Purpose: Ensures business continuity and data recovery in case of failure.

   Configuration:

   (a) For Odoo.sh: Backups are automatic (daily + on deploy)

   (b) For on-premise:

      i. Schedule daily database dumps via cron

      ii. Store backups offsite (encrypted)

      iii. Test restore quarterly

   (c) Document recovery procedure (RTO/RPO)

   Critical: Backups include all user data, configurations, and file attachments.

8.2 The Governance Logic Behind Key Administrative Features

Odoo's Administrative Management framework isn't just about creating users or importing data—it's built on core principles of security, compliance, data integrity, and least-privilege access. Understanding the governance logic behind its key features helps your team configure the system securely, prevent unauthorized access, and maintain audit readiness.

Below, we break down the purpose, administrative rationale, and practical impact of Odoo's most important administrative features.

1. **Centralized User and Group Management**

   What It Is: A unified interface to create users and assign them to security groups that control access across all Odoo modules.

   Governance Logic:

(a) Enforces a **single source of truth** for identity and permissions—no siloed access controls per app.

(b) Supports the **principle of least privilege**: users only see and modify what their role requires.

(c) Required by ISO 27001, SOC 2, and GDPR for access control and segregation of duties.

Example: A Sales user assigned to the *Sales / User* group can create quotations and view their own customers—but cannot access HR employee records or approve vendor bills.

Result: Reduced risk of data leakage, insider threats, and accidental changes.

2. **Automatic User–Employee Linking**

What It Is: When an employee is created in the HR app, Odoo can automatically generate a corresponding user account.

Governance Logic:

(a) Eliminates manual, error-prone user provisioning workflows.

(b) Ensures immediate access for new hires—improving productivity.

(c) Synchronizes offboarding: archiving an employee can deactivate their login, reducing orphaned accounts.

Impact:

(a) HR and IT teams operate from a single workflow.

(b) Audit trails show clear lineage: "User created because Employee X was hired."

3. **Record Rules for Data Isolation**

What It Is: Database-level filters that restrict which records a user can see or edit—even within the same group.

Governance Logic:

(a) Goes beyond menu-level security to enforce **row-level access control**.

(b) Critical in multi-tenant, multi-company, or departmental environments.

(c) Prevents users from bypassing UI restrictions via API or direct model access.

Real-World Need:

(a) A sales rep in "Team A" should not see leads assigned to "Team B."

(b) A user in "Company France" must not see invoices from "Company Germany."

Result: True data segregation without custom development.

4. **Data Import/Export Engine with Permission Enforcement**

   What It Is: A native tool in every list view to bulk import or export data—automatically respecting the user's access rights.

   Governance Logic:

   (a) Ensures that **security follows data**: users cannot export records they can't view in the UI.

   (b) Prevents accidental or malicious data exfiltration.

   (c) Supports compliance with data minimization principles (e.g., GDPR Article 5).

   Example:

   (a) An HR officer exports employee data → only sees employees in their department.

   (b) A regional manager imports contacts → cannot create records in a company they don't belong to.

   Critical for: Secure data migration, reporting, and third-party integrations.

5. **External Authentication (SSO) Integration**

   What It Is: Native support for LDAP, OAuth, and SAML to delegate login to enterprise identity providers.

   Governance Logic:

   (a) Centralizes identity management—users log in once, access multiple systems.

   (b) Enforces corporate password policies, MFA, and session controls.

   (c) Simplifies compliance with security frameworks (NIST, CIS Controls).

   Example:

   (a) An employee leaves the company → their Active Directory account is disabled → immediate loss of Odoo access.

   Impact: Eliminates local password sprawl and strengthens perimeter security.

6. **Audit Logging (Odoo Enterprise)**

   What It Is: Automatic tracking of user actions (creates, updates, logins) with full context.

   Governance Logic:

   (a) Provides non-repudiation: every change is tied to a user, timestamp, and IP address.

   (b) Enables forensic investigation during security incidents.

   (c) Required for SOX, GDPR, and HIPAA compliance.

   Business Impact:

   (a) Detect when a user was granted admin rights unexpectedly.

(b) Prove during an audit that sensitive data was not accessed improperly.

7. **Multi-Company Data Isolation**

   What It Is: Built-in architecture that separates data by legal entity or operating unit.

   Governance Logic:

   (a) Ensures financial and operational data privacy between subsidiaries.

   (b) Prevents cross-contamination of configurations (e.g., taxes, charts of accounts).

   (c) Supports legal requirements for data residency and entity separation.

   Workflow:

   (a) User assigned to "Company A" → sees only Company A data by default.

   (b) Admins with access to multiple companies can switch context—but actions are logged.

   Once configured, isolation is enforced at the database level—no override without explicit permission.

8. **User Lifecycle Management**

   What It Is: Standardized processes for onboarding (create/invite), role changes (group updates), and offboarding (archive/deactivate).

   Governance Logic:

   (a) Reduces attack surface by ensuring timely access revocation.

   (b) Creates a clear audit trail of access changes over time.

   (c) Supports role-based access reviews (RBAC audits).

   Best Practice:

   (a) Archive (don't delete) users to preserve historical data integrity.

   (b) Review inactive accounts monthly; auto-deactivate after 90 days.

9. **Developer Mode Controls**

   What It Is: A privileged mode that exposes technical settings (record rules, model fields, XML views).

   Governance Logic:

   (a) Must be restricted to system administrators only.

   (b) Prevents accidental misconfiguration of security or data models.

   (c) Changes made in Developer Mode should be documented and reviewed.

   Security Note: Never enable Developer Mode for end-users or in production without strict access controls.

10. **Backup and Recovery as a Governance Control**

    What It Is: Regular, automated backups of the database and filestore.

    Governance Logic:

    (a) Ensures business continuity and data availability (CIA triad: Confidentiality, Integrity, Availability).

    (b) Allows rollback after configuration errors or malicious changes.

    (c) Part of disaster recovery and incident response plans.

    Example: After an accidental mass deletion of users, restore from yesterday's backup—minimizing downtime.

    Critical for: All organizations, especially those subject to operational resilience regulations.

Chapter 9

Master Data: Schema and Structure

9.1 Understanding the Code and Class Structure

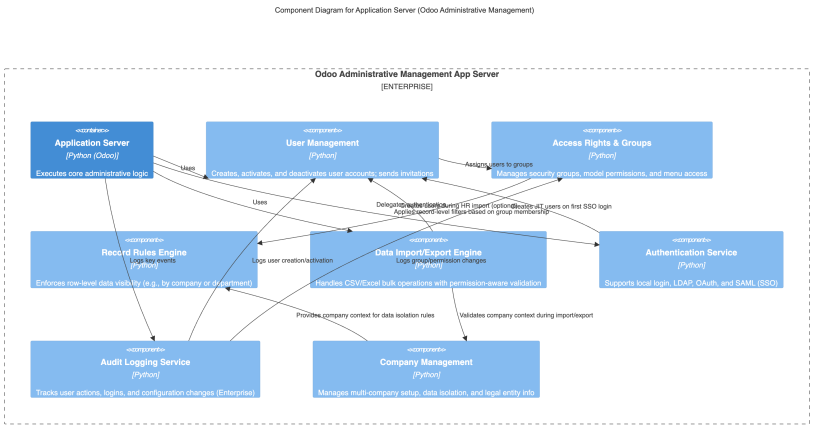

Figure 9.1: C3 Diagram of Odoo Accounting Module

This component diagram provides a high-level description of the Odoo Administrative Management framework, breaking it down into its primary functional components and how they interact to enforce secure, compliant, and efficient user and data governance. Each component embodies a specific set of duties that collectively enable end-to-end administrative control across the Odoo system.

1. **User Management**

   Description: Manages the full lifecycle of system users—from creation and activation to deactivation and archival.

   Key Responsibilities:

   (a) Create, update, and archive user accounts.

   (b) Send secure invitation emails with setup links.

   (c) Link users to companies and job positions (in multi-company setups).

   (d) Support auto-creation from HR employee records.

   Interfaces:

(a) Create and fetch user data via UI or API.

(b) Trigger authentication workflows (local or SSO).

Dependencies:

(a) **Access Rights & Groups** – to assign permissions after creation.

(b) **Authentication Service** – to handle login and identity verification.

(c) **Audit Logging Service** – to log user provisioning events.

2. **Access Rights & Groups**

Description: Central engine for role-based access control (RBAC) across all Odoo modules.

Key Responsibilities:

(a) Define security groups (e.g., *Sales / User*, *HR / Officer*).

(b) Manage model-level permissions (read/write/create/delete).

(c) Control menu visibility per group.

Interfaces:

(a) Assign users to groups.

(b) Query effective permissions for a given user.

Dependencies:

(a) **Record Rules Engine** – to enforce row-level data filters based on group membership.

(b) **Audit Logging Service** – to track permission changes.

3. **Record Rules Engine**

Description: Enforces fine-grained, row-level data visibility and modification rules.

Key Responsibilities:

(a) Apply domain filters (e.g., `[('company_id', '=', user.company_id.id)]`).

(b) Restrict access to records based on user attributes (company, department, role).

(c) Operate at the ORM/database level—bypassing UI restrictions.

Interfaces:

(a) Define and maintain record rules via technical settings.

(b) Evaluate rules dynamically during data queries.

Dependencies:

(a) **Company Management** – to resolve company context for isolation.

(b) **Access Rights & Groups** – to link rules to user groups.

4. **Data Import/Export Engine**

   Description: Handles bulk data operations while respecting user permissions and data integrity.

   Key Responsibilities:

   (a) Import CSV/Excel files into any Odoo model (Users, Contacts, Products, etc.).

   (b) Export filtered data sets based on the user's access rights.

   (c) Validate field mappings, data types, and required constraints.

   (d) Use External IDs to update existing records reliably.

   Interfaces:

   (a) Upload/download files via list views.

   (b) Map source columns to Odoo fields.

   Dependencies:

   (a) **User Management** – to validate importer identity and rights.

   (b) **Record Rules Engine** – to filter export results.

   (c) **Company Management** – to validate company context during import.

5. **Authentication Service**

   Description: Manages user identity verification and single sign-on (SSO) integration.

   Key Responsibilities:

   (a) Support local password-based login.

   (b) Integrate with external identity providers (LDAP, OAuth, SAML).

   (c) Enable Just-in-Time (JIT) user provisioning on first SSO login.

   (d) Enforce session timeouts and 2FA (Enterprise).

   Interfaces:

   (a) Authenticate credentials against internal or external providers.

   (b) Return user context and session token.

   Dependencies:

   (a) **User Management** – to create or activate users during JIT flow.

   (b) **Audit Logging Service** – to log login attempts and session activity.

6. **Audit Logging Service (Odoo Enterprise)**

   Description: Provides immutable tracking of administrative actions for compliance and security.

   Key Responsibilities:

   (a) Log user creations, group assignments, and permission changes.

   (b) Track data imports, exports, and record modifications.

   (c) Record IP address, timestamp, and before/after field values.

   Interfaces:

   (a) Query audit logs by user, date, model, or action.

   (b) Export logs for archival or external review.

   Dependencies:

   (a) **User Management**, **Access Rights**, **Data Import/Export Engine** – as sources of auditable events.

7. **Company Management**

   Description: Manages legal entities and enforces data isolation in multi-company environments.

   Key Responsibilities:

   (a) Define company records (name, address, logo, currency).

   (b) Assign users to one or more companies.

   (c) Enable and configure multi-company mode.

   Interfaces:

   (a) Create and update company details.

   (b) Switch user context between companies (for admins).

   Dependencies:

   (a) **Record Rules Engine** – to apply company-based data filters.

   (b) **Data Import/Export Engine** – to validate company during bulk operations.

This diagram illustrates the core components of Odoo's administrative governance layer and their interactions. The User Management component (res.users) manages the full identity lifecycle—including user creation, invitation, and archival—and links users to one or more legal entities via Company Management (res.company). Access Rights & Groups (res.groups) defines role-based permissions for menus and model-level operations (read/write/create/delete), while the Record Rules Engine (ir.rule) enforces row-level data visibility (e.g., "users see only records from their company"), ensuring true least-privilege access.

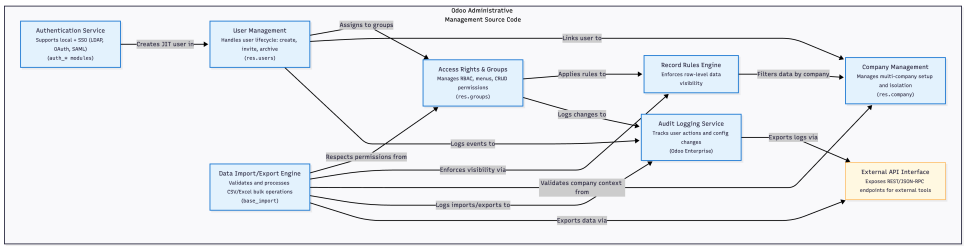

Figure 9.2: C4 Diagram of Odoo Administrative Management Framework

The Data Import/Export Engine (base_import) enables secure bulk data operations across all modules; it validates field mappings, respects the current user's access rights, and filters exports using the same record rules applied in the user interface. Authentication is handled by the Authentication Service, which supports local login as well as enterprise single sign-on (SSO) via LDAP, OAuth, or SAML—and can automatically provision users on first login (JIT provisioning).

All sensitive actions—such as user creation, group assignment, and data imports/exports—are captured by the Audit Logging Service (Odoo Enterprise) to provide a complete, tamper-resistant audit trail. Finally, the External API Interface exposes REST/JSON-RPC endpoints, allowing authorized third-party tools to securely retrieve audit logs, user data, or exported records—always respecting Odoo's built-in permission model.

Together, these components form a cohesive, secure, and scalable administrative backbone that governs identity, data, and access across the entire Odoo ecosystem—regardless of which business applications (Sales, HR, Accounting, etc.) are deployed.

9.2 Master Data Schema

Core Tables

Table (Model)	Description
`res.users`	Core user table; stores login, email, status (active/archived), and company affiliations.
`res.groups`	Defines security groups (e.g., *Sales / User*, *HR / Officer*); controls menu access and model-level permissions (read/write/create/delete).
`ir.rule`	Stores record rules that enforce row-level data visibility (e.g., "user sees only their company's records"). Applied at the ORM level for all queries.
`res.company`	Holds legal entity data (name, address, logo, currency); enables multi-company setups and data isolation.
`res.partner`	Stores contacts (customers, vendors, employees); links to `res.users` when a contact is a system user.
`ir.model.access`	Defines access control lists (ACLs) for models—grants CRUD permissions to groups or users.
`ir.attachment`	Stores file attachments (e.g., imported CSVs, exported reports); access is governed by record rules and ownership.
`base_import.import`	Internal model used by the Data Import Engine to manage CSV/Excel upload sessions and field mappings.
`ir.logging`	(Odoo Enterprise) Stores audit log entries—captures user actions, field changes, timestamps, and IP addresses.
`auth.oauth.provider`	Configuration for OAuth 2.0 identity providers (e.g., Google, Azure AD).
`auth.ldap`	Stores LDAP server settings for Active Directory or OpenLDAP integration.
`ir.config_parameter`	System-wide configuration parameters (e.g., session timeout, SSO settings, import/export options).
`ir.ui.menu`	Defines application menus; visibility is controlled by security groups via `groups_id`.
`ir.actions.act_window`	Window actions that open views; access can be restricted via groups.
`res.users.log`	Tracks user login sessions (timestamp, IP address); available in Odoo Community and Enterprise.
`ir.exports`	Stores user-defined export templates (field selections for recurring data exports).
`ir.exports.line`	Defines individual fields within an export template.

`ir.sequence`	Manages document numbering sequences (e.g., user IDs, import batch IDs).

Table 9.1: Core Administrative Data Tables in Odoo

Chapter 10

Reporting, Dashboards, and Analytics

10.1 Key Performance Indicators (KPIs) for Administrative Governance

Key Performance Indicators (KPIs) are measurable values that demonstrate how effectively an organization manages its **administrative governance**: user access, data security, compliance, and system integrity. In Odoo, these KPIs provide real-time insights into identity lifecycle efficiency, permission hygiene, data handling accuracy, and audit readiness.

Odoo's integrated administrative framework ensures these KPIs can be tracked using native logs, user reports, and configuration audits—eliminating manual reviews and enabling proactive risk management.

Core Administrative Governance KPIs in Odoo

The following KPIs can be monitored using built-in features or simple custom reports—no third-party tools required:

1. **User Provisioning Time**

   Definition: Average time from HR request to active user account.

   Odoo Source:

   (a) Compare `employee.create_date` (HR) with `res.users.create_date`

   (b) Or track invitation send vs. first login (via `res.users.log`)

   Why It Matters: Slow onboarding delays productivity and increases IT workload.

2. **Inactive User Rate**

   Definition: Percentage of active users who have not logged in for >90 days.

   Formula:
   $$\frac{\text{Number of active users with no login in last 90 days}}{\text{Total active users}} \times 100$$

   Odoo Source:

   (a) `res.users` (filter by `active = True`)

(b) `res.users.log` (last login timestamp)

Why It Matters: High inactive rate increases security risk and license costs.

3. **Orphaned Account Count**

   Definition: Number of user accounts not linked to an active employee or partner.

   Odoo Source:

   (a) Users where `employee_ids` is empty and `partner_id` is not a vendor/customer

   (b) Common for test, service, or legacy accounts

   Why It Matters: Orphaned accounts are high-risk attack vectors.

4. **Excessive Permission Rate**

   Definition: Percentage of users assigned to high-privilege groups (e.g., *Settings*, *Administrator*) without documented justification.

   Odoo Source:

   (a) `res.users` → `groups_id`

   (b) Flag users in groups like `base.group_system` or `account.group_account_manager`

   Why It Matters: Violates least-privilege principle; increases insider threat risk.

5. **Data Import Success Rate**

   Definition: Percentage of import attempts that complete without errors.

   Formula:

$$\frac{\text{Successful imports}}{\text{Total import attempts}} \times 100$$

   Odoo Source:

   (a) Review import logs (via `base_import.import` or UI feedback)

   (b) Track repeated failures for specific users or models

   Why It Matters: Low success rate indicates poor data quality or insufficient user training.

6. **Export Volume by User Role**

   Definition: Frequency and volume of data exports by user group (e.g., HR vs. Sales).

   Odoo Source:

   (a) Audit logs (Odoo Enterprise: `ir.logging`)

   (b) Or track usage of `ir.exports` and export actions

   Why It Matters: Unusual export patterns may signal data exfiltration or policy violations.

7. **SSO Adoption Rate**

   Definition: Percentage of logins using external authentication (LDAP, OAuth, SAML) vs. local passwords.

   Formula:

$$\frac{\text{SSO logins in period}}{\text{Total logins in period}} \times 100$$

   Odoo Source:

   (a) `res.users.log` (check authentication method if logged)

   (b) Proxy or IdP logs (for precise tracking)

   Why It Matters: Higher SSO adoption improves security and reduces password fatigue.

8. **Multi-Company Data Leak Incidents**

   Definition: Number of records incorrectly visible across company boundaries.

   Odoo Source:

   (a) Test via user impersonation: can User A (Company A) see records from Company B?

   (b) Validate `ir.rule` configurations for core models (`res.partner`, `account.move`, etc.)

   Why It Matters: Data leaks violate legal and compliance requirements (e.g., GDPR, SOX).

9. **Audit Log Coverage**

   Definition: Percentage of critical administrative actions captured in audit logs.

   Odoo Source:

   (a) Odoo Enterprise: `ir.logging` should include user creation, group changes, data exports

   (b) Verify logs exist for all high-risk operations

   Why It Matters: Incomplete logs undermine forensic investigations and compliance audits.

Accessing Governance KPIs in Odoo

1. **User Reports**

   (a) `Settings → Users & Companies → Users`

   (b) Filter by last login, company, or group to assess provisioning and activity

2. **Audit Logs (Enterprise)**

   (a) `Settings → Technical → Logs → Audit Logs`

(b) Export to analyze permission changes, data exports, and configuration updates

3. **Custom KPI Dashboards**

   (a) Use Odoo Studio (Enterprise) or custom modules to:

      i. Build pivot tables of user activity

      ii. Set alerts (e.g., "Notify if admin group assignment occurs")

      iii. Visualize inactive user trends

4. **Access Reviews**

   (a) Schedule quarterly reviews of:

      i. Users in high-privilege groups

      ii. Orphaned or inactive accounts

      iii. Record rules for sensitive models

   (b) Document approvals and cleanup actions

Example: Setting Up an Inactive User Alert

1. Create a scheduled action (via `Settings → Technical → Automation → Scheduled Actions`)
2. Query `res.users` where `login_date < today - 90 days` and `active = True`
3. Send weekly email to IT admin with list of stale accounts
4. Archive accounts after 120 days of inactivity

These KPIs empower System Administrators, Compliance Officers, and IT Managers to maintain a **secure, efficient, and auditable** Odoo environment—ensuring that governance keeps pace with business growth.

10.2 Available Administrative Reports and Dashboards

Odoo provides a comprehensive set of built-in administrative reports and dashboards that give System Administrators, HR Managers, and Compliance Officers full visibility into user activity, access control, data operations, and system health. These tools are generated from live system data—ensuring accuracy, enabling proactive governance, and supporting audit readiness.

Most reports are accessible via `Settings → Users & Companies`, `Settings → Technical`, or module-specific menus, and can be filtered by date, user, company, or group.

User and Access Management Reports These reports help maintain secure, efficient, and compliant user governance.

1. **User List and Activity Summary**

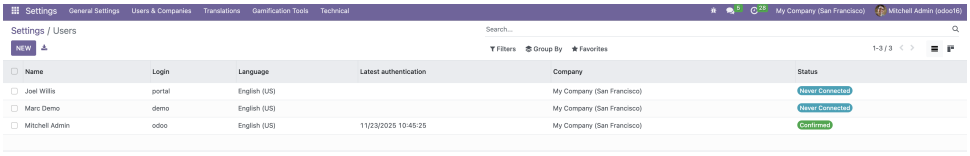

Figure 10.1: User List with Status and Login History

Purpose: View all users, their status (active/archived), assigned groups, company, and last login date.

Path: `Settings → Users & Companies → Users`

Features:

(a) Filter by group (e.g., "Show all Admins")

(b) Sort by last login to identify inactive accounts

(c) Export to Excel for access reviews

Use Case: Quarterly access certification, offboarding validation, or license optimization.

2. **Security Groups and Permissions Report**

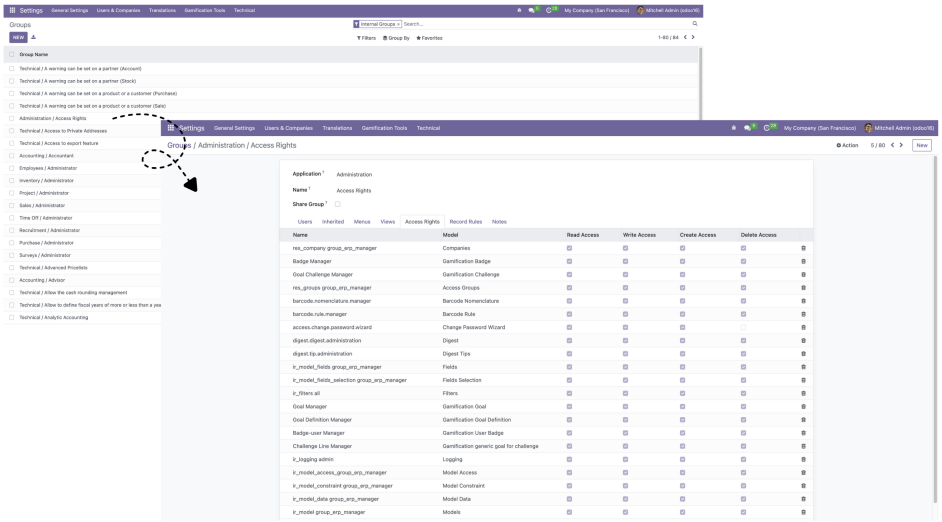

Figure 10.2: Security Groups and Assigned Users

Purpose: Review which users belong to each security group and what permissions the group grants.

Path: `Settings → Users & Companies → Groups`

Features:

(a) Click any group to see its access rights (menus, model permissions)

(b) View member list with names and companies

(c) Identify over-provisioned groups (e.g., too many "Settings" users)

Use Case: Enforce least-privilege access and prepare for internal audits.

3. **Login Activity Log**

   Purpose: Track user sign-ins, including timestamp and (in some configurations) IP address.

   Path: `Settings → Users & Companies → Users` → Open user → `Log` tab (Also visible in `res.users.log` model via Developer Mode)

   Use Case: Detect suspicious logins (e.g., unusual time/location) or verify onboarding completion.

Data Governance and Operational Reports These reports support secure, accurate bulk data handling and system integrity.

1. **Data Import/Export History**

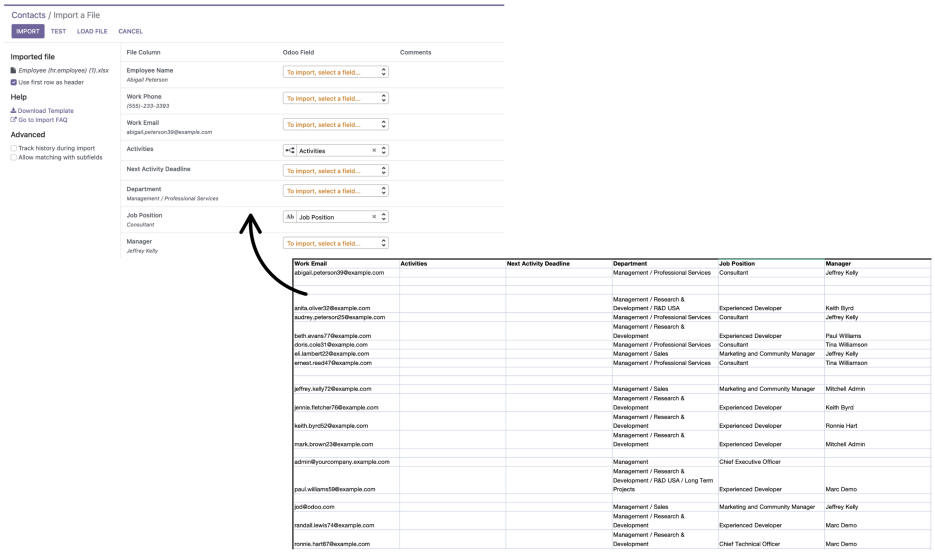

Figure 10.3: Data Import/Export Activity

Purpose: Monitor who imported or exported data, when, and what type of records were affected.

Path:

(a) `Settings → Technical → Sequences & Identifiers → External Identifiers` (for import tracking)

(b) Or use `ir.exports` to view saved export templates

(c) (Odoo Enterprise) `Settings → Technical → Logs → Audit Logs` for full data export trails

Use Case: Investigate data leaks, validate bulk operations, or comply with data access requests (e.g., GDPR).

2. **Record Rules Validation Report**

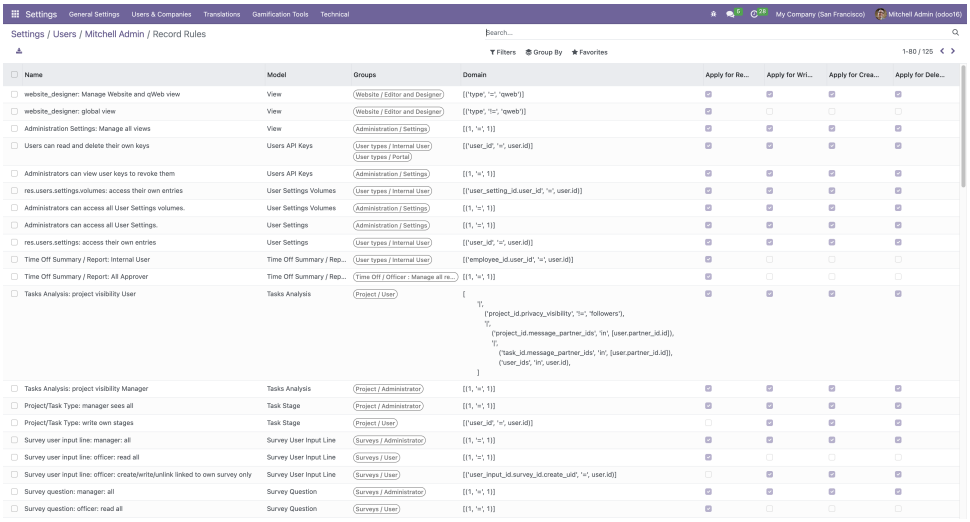

Figure 10.4: Record Rules Overview

Purpose: Review active record rules that control data visibility across models.

Path: `Settings → Activate Developer Mode → Settings → Technical → Security → Record Rules`

Details:

(a) Shows domain filters (e.g., `[('company_id', '=', user.company_id.id)]`)

(b) Lists associated groups and affected models

Use Case: Verify multi-company isolation or troubleshoot "missing records" reported by users.

3. **Company and Multi-Entity Configuration Report**

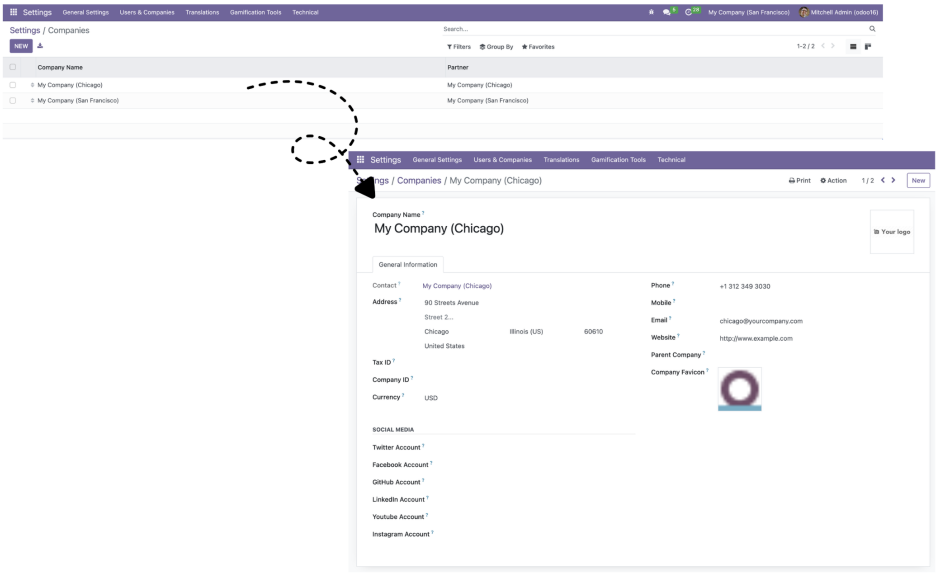

Figure 10.5: Company Configuration Overview

Path: `Settings → Users & Companies → Companies`

Details: Lists all legal entities, their currency, logo, and tax ID.

Use Case: Ensure correct company setup before onboarding users or enabling multi-company mode.

Compliance and Audit Reports (Odoo Enterprise) For organizations requiring formal compliance evidence.

1. **Audit Log Report**

   Purpose: Immutable record of critical system changes—user creation, permission updates, data exports, etc.

   Path: `Settings → Technical → Logs → Audit Logs`

   Features:

   (a) Filter by user, date, model (e.g., `res.users`, `ir.rule`)

   (b) View field changes (before/after values)

   (c) Export full log for external audit

   Use Case: SOX, GDPR, or ISO 27001 compliance; forensic investigations.

2. **Authentication and SSO Configuration Report**

   Purpose: Document external identity provider settings (LDAP, OAuth, SAML).

   Path: `Settings → Activate Developer Mode` → `Settings → Technical → Authentication`

   Use Case: Security review, incident response, or third-party assurance.

These administrative reports and dashboards empower your team to maintain a **secure, transparent, and compliant** Odoo environment—ensuring that governance is not an afterthought, but a continuous, data-driven practice.

10.3 Mastering Default Groups and Filters for Administrative Views

Odoo provides powerful grouping and filtering tools that allow administrators to organize, analyze, and act on user, access, and data governance information quickly—without spreadsheets or manual reviews. These features are available in key administrative list views (e.g., Users, Groups, Companies, Audit Logs) and are essential for onboarding, access reviews, compliance audits, and system monitoring.

Understanding how to use default groups and custom filters improves operational efficiency, reduces security risks, and enables proactive governance.

What Are Groups and Filters?

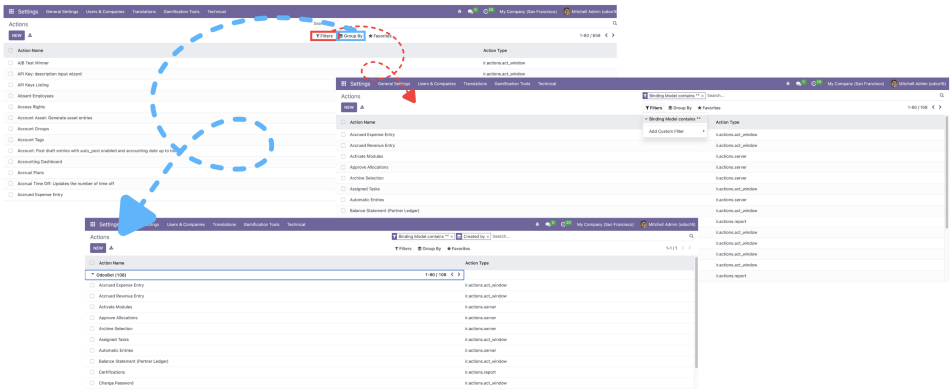

Figure 10.6: Group & Filter in Odoo Administrative Views

Filters: Narrow down records based on criteria (e.g., "Inactive," "Last Login > 90 Days Ago," "Assigned to HR Group").

Groups: Organize records into collapsible sections by a field (e.g., group users by Company, Status, or Security Group).

Default Filters in Key Administrative Views Odoo provides smart, context-aware default filters to help you focus on high-priority administrative tasks.

1. **Users**

   Default Filters:

   (a) **Active**: Currently enabled accounts

   (b) **Archived**: Deactivated accounts (offboarded users)

   (c) **Internal Users**: Excludes portal/partner users

   (d) **Employees**: Users linked to an HR employee record

   Use Case: Quickly identify users needing offboarding or audit for orphaned accounts.

2. **Security Groups**

   Default Filters:

   (a) **Application Groups**: Groups tied to specific apps (e.g., Sales, HR)

   (b) **Custom Groups**: User-defined permission sets

   (c) **Groups with Users**: Hide empty groups

   Use Case: Review which groups are actively used and clean up obsolete ones.

3. **Companies**

   Default Filters:

   (a) **My Company**: Your primary entity

   (b) **All Companies**: In multi-company setups

Use Case: Verify company setup before user provisioning.

4. **Audit Logs (Odoo Enterprise)**

   Default Filters:

   (a) **Today / This Week / This Month**

   (b) **User Creation**

   (c) **Group Assignment**

   (d) **Data Export**

   Use Case: Monitor high-risk events in real time during security investigations.

Tip: Click the funnel icon (FilterWhere) next to the search bar to see all available default filters. All are accessible via the search bar at the top of any list view in Odoo.

Default Groupings Grouping helps visualize administrative data hierarchically. Odoo applies sensible defaults to support common workflows.

View	Default Group By	Purpose
Users	Company	See all users per legal entity (critical in multi-company setups)
Users	Status	Separate active vs. archived users
Security Groups	Application	Organize groups by module (Sales, HR, Accounting, etc.)
Audit Logs	User	Track all actions performed by a specific administrator
Companies	Currency	Group entities by reporting currency

Table 10.1: Default Groupings in Odoo Administrative Views

How to Change Grouping

1. Open any administrative list view (e.g., `Settings → Users & Companies → Users`).
2. Click the **Group By** button (top-right, next to search bar).
3. Select a field (e.g., *Last Login*, *Security Group*, *Company*).
4. Records instantly reorganize into collapsible sections.

Tip: You can apply multiple levels of grouping (e.g., Group by Company, then by Security Group) by clicking **Group By** again after the first grouping.

Creating and Saving Custom Filters

Step-by-Step: Create a Custom Filter

1. In any list view, click the **Filters** dropdown (funnel icon).
2. Select **Add Custom Filter**.

3. Choose a field (e.g., *Last Login*), operator (e.g., *is less than*), and value (e.g., *90 days ago*).
4. Click **Apply**.

Example Custom Filters

- **Stale Accounts:** Status = Active + Last Login < 90 Days Ago
- **Privileged Users:** Security Group = Settings (or group_system)
- **HR-Managed Users:** Company = "Main Corp" + Security Group = HR / Officer
- **Recent Data Exports (Enterprise):** Model = ir.exports + Date > 7 Days Ago

Saving Filters for Reuse

1. After applying a custom filter, click **Save Current Filter**.
2. Give it a descriptive name (e.g., "Inactive Users – Review").
3. It will appear under **Favorites** for one-click access.

Note: Saved filters are personal by default. Administrators can share them globally via `Settings → Technical → User-defined Filters` (Odoo Enterprise).

These tools empower your team to maintain a **secure, efficient, and auditable** administrative environment—turning raw system data into actionable governance insights with just a few clicks.

Part V

Governance and Enablement

Chapter 11

Governance: User Roles and Access Rights

11.1 Defining Administrative User Roles: Viewer, Operator, and Administrator

Odoo uses a role-based access control (RBAC) system to ensure data security, operational efficiency, and compliance across all modules. In the context of **Administrative Management**, user roles determine who can view, create, modify, or manage system configurations, user accounts, data operations, and audit settings.

While Odoo provides granular control via groups and record rules, most administrative responsibilities can be mapped to three practical roles:

- **Viewer** (Read-Only Access)
- **Operator** (Standard Admin / Data Steward)
- **Administrator** (System Owner / Compliance Officer)

Understanding these roles helps organizations enforce least-privilege access while maintaining system integrity and audit readiness.

Role Definitions & Permissions

1. **Viewer (Read-Only Access)**

   Typical Users: Internal auditors, department managers, compliance reviewers, or external assessors.

   Access Level: View-only access to administrative data—no ability to modify users, permissions, or configurations.

   Permissions:

   (a) View active users, their assigned groups, and company affiliations

   (b) See security group definitions and associated permissions

   (c) Access company information (name, address, currency)

   (d) View saved export templates and import history (if permitted)

(e) Cannot create, edit, archive users, or change access rights

(f) Cannot trigger data imports or exports

Odoo Groups:

(a) Custom group (e.g., *Admin / Viewer*) with read-only access to:

i. `res.users`

ii. `res.groups`

iii. `res.company`

(b) No access to `Settings` or `Technical` menus

Use Case: A department manager needs to verify which team members have access to HR data but must not be able to grant or revoke permissions.

Tip: In Odoo Enterprise, consider using **Portal Access** or restricted internal users to avoid consuming full user licenses for read-only reviewers.

2. **Operator (Standard Admin / Data Steward)**

Typical Users: HR coordinators, IT support staff, data migration specialists, or onboarding officers.

Access Level: Full operational access to user management and data operations—but **not** system configuration or audit log access.

Permissions:

(a) Create, activate, and archive user accounts

(b) Assign users to predefined security groups (e.g., Sales / User, HR / Officer)

(c) Import and export master data (Contacts, Users, Products) via CSV/Excel

(d) View company details and switch between assigned companies

(e) Use saved export templates

(f) Cannot create or modify security groups, record rules, or authentication settings

(g) Cannot access audit logs or Developer Mode

(h) Cannot change system-wide parameters (e.g., session timeout, SSO config)

Odoo Groups:

(a) `base.group_user` (Internal User)

(b) Custom group: *Admin / User Manager* (grants CRUD on `res.users`)

(c) Access to `base_import` (Data Import/Export Engine)

Use Case: An HR coordinator onboards new hires by creating user accounts and assigning them to the "Employees" and "HR / User" groups—but cannot grant administrator rights.

Best Practice: Never assign the `Settings` or `Administration` groups to Operators—this prevents accidental system changes.

3. **Administrator (System Owner / Compliance Officer)**

   Typical Users: System administrators, CISOs, compliance officers, or ERP managers.

   Access Level: Full access to all administrative data, configurations, and audit capabilities.

   Permissions:

   (a) All Operator capabilities

   (b) Create, edit, and delete security groups and record rules

   (c) Configure external authentication (LDAP, OAuth, SAML)

   (d) Manage multi-company settings and data isolation rules

   (e) Access and export audit logs (Odoo Enterprise)

   (f) Modify system parameters (e.g., session timeout, password policy)

   (g) Activate Developer Mode and access technical settings

   (h) Install or customize administrative modules

   (i) Perform access reviews and permission audits

   Odoo Groups:

   (a) `base.group_system` (Administration → Settings)

   (b) `base.group_technical_features` (Developer Mode)

   (c) (Enterprise) `auditlog.group_auditlog_manager`

   Use Case: A system administrator configures SSO with Azure AD, defines record rules for multi-company isolation, and exports audit logs for a SOC 2 review.

   Security Note: The `base.group_system` role grants unrestricted access to the entire database. Assign it only to highly trusted personnel and monitor usage via audit logs.

How to Assign Administrative Roles in Odoo

1. Go to `Settings → Users & Companies → Users`.
2. Open a user record.
3. Under **Access Rights**, assign the appropriate groups:
   (a) For **Viewer**: Create a custom read-only group (via Developer Mode) or use a minimal internal user profile.
   (b) For **Operator**: Enable `Internal User` + custom *User Manager* group + `base_import` access.
   (c) For **Administrator**: Enable `Administration → Settings` and `Technical Features`.
4. Save the user.

Advanced Control (Odoo Enterprise): Use **Odoo Studio** or custom modules to define fine-grained roles (e.g., "Can import users but not export," "Can view audit logs but not modify SSO settings"). This enables precise alignment with your organization's segregation-of-duties policy.

11.2 Access Rights Matrix: A Clear Table of Administrative Permissions

Odoo uses a granular role-based access control (RBAC) system to manage administrative permissions. While high-level roles like *Operator* or *Administrator* provide a useful abstraction, this Access Rights Matrix details exact permissions across core administrative operations.

This matrix helps you:

- Assign appropriate access during onboarding
- Conduct internal compliance or access reviews
- Troubleshoot permission-related issues
- Enforce segregation of duties (SoD) for IT and HR functions

Note: Permissions are controlled via security groups (e.g., `base.group_user`, `base.group_system`) and record rules. The matrix below maps real-world administrative roles to these technical controls.

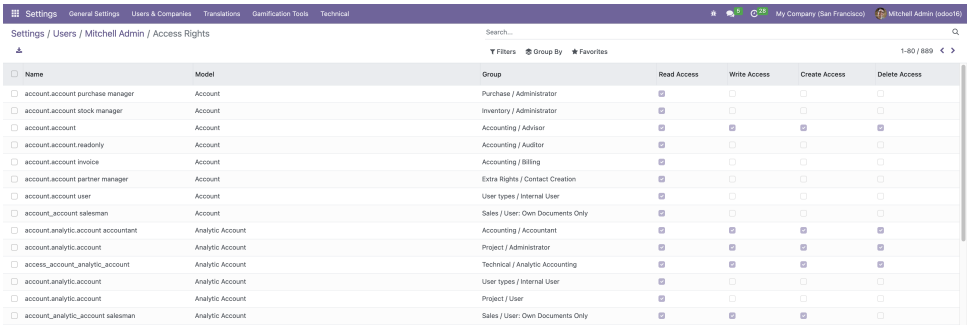

Figure 11.1: Administrative Access Rights in Odoo

Access Rights Matrix for Administrative Roles

Administrative Operation	Viewer	Operator	Administrator
View active users (name, email, company)	Yes	Yes	Yes
View user login history (last login)	Yes	Yes	Yes
View archived/inactive users	No	Yes	Yes
Create new user accounts	No	Yes	Yes

Send user invitation emails	No	Yes	Yes
Archive/deactivate user accounts	No	Yes	Yes
Assign users to security groups	No	Yes	Yes
Remove users from security groups	No	Yes	Yes
View security group definitions (menus, model access)	Yes	Yes	Yes
Create/edit security groups	No	No	Yes
View record rules (data visibility filters)	No	No	Yes
Create/edit record rules	No	No	Yes
Import data (CSV/Excel) into any model	No	Yes	Yes
Export data (filtered by user permissions)	Conditional*	Yes	Yes
Save custom export templates	No	Yes	Yes
View company information (name, address, logo)	Yes	Yes	Yes
Edit company information	No	No	Yes
Manage multi-company assignments for users	No	Yes	Yes
Configure LDAP/Active Directory integration	No	No	Yes
Configure OAuth/SAML (SSO) providers	No	No	Yes
Enable Developer Mode	No	No	Yes
Access Technical Settings (e.g., `ir.rule`, `ir.model.access`)	No	No	Yes
View audit logs (user actions, logins, exports)	No	No	Yes
Export audit logs	No	No	Yes
Modify system parameters (e.g., session timeout)	No	No	Yes
Install/uninstall apps or modules	No	No	Yes
Manage user-defined filters and dashboards	No	Yes	Yes
Impersonate other users (for testing)	No	No	Yes

Table 11.1: Access Rights Matrix for Odoo Administrative Roles

Chapter 12

Learning and Development Resources

12.1 Official Odoo Documentation and Video Tutorials

Official Odoo Administrative Documentation The official Odoo documentation is your primary source for detailed instructions on user management, access control, data handling, and system configuration.

Odoo 16 Administration Documentation (Latest Stable Version) https://www.odoo.com/documentation/16.0/administration.html

This section covers:

- User and company management
- Security groups and access rights
- Record rules and data isolation
- Multi-company configuration
- Authentication (LDAP, OAuth, SAML)
- Data import and export
- Audit logging (Enterprise)
- Developer Mode and technical settings

Tip: Always select the documentation version that matches your Odoo installation (e.g., 16.0, 17.0). Use the version dropdown at the top of the documentation page.

Official Odoo Video Tutorials

Odoo provides high-quality, step-by-step video tutorials on its official YouTube channel and eLearning platform—ideal for visual learners and system administrators.

Cybrosys Technologies YouTube Channel – Groups and Access Rights in Odoo https://www.youtube.com/watch?v=PmSepSujsBk (Search for "Odoo User Management", "Odoo Security", or "Odoo Multi-Company")

Odoo eLearning Platform (Free Courses) https://www.odoo.com/slides/getting-started-15 → Browse under "Administration" and "Security" for interactive courses, including:

- Managing Users and Companies
- Configuring Access Rights and Record Rules
- Setting Up SSO with LDAP or OAuth
- Importing and Exporting Data

Note: The eLearning platform includes quizzes and downloadable guides to reinforce learning.

Odoo Community & Support

For questions beyond the documentation:

- **Odoo Forum:** https://www.odoo.com/forum/help-1 (Use tags: `security`, `users`, `import`, `multi-company`)
- **GitHub Issues (Community Edition):** https://github.com/odoo/odoo/issues (Filter by labels: `access rights`, `users`, `import`)

Enterprise users receive direct support via the Odoo Support portal or their account manager.

12.2 Community Forums and Learning Paths

While official documentation provides foundational knowledge, engaging with the Odoo community and following structured learning paths can significantly accelerate your proficiency in administrative governance. Below are trusted resources and curated learning journeys for Odoo 16.

1. **Odoo Community Forums**

   The Odoo Community Forum is a vibrant space where administrators, developers, and consultants share solutions for user management, security, and data governance.

2. **Odoo Help Forum (Official)**
   https://www.odoo.com/forum/help-1

   - Search for topics like “record rules not working”, “SSO setup”, or “user import fails”.
   - Filter by version (Odoo 16) and tags (`security`, `users`, `import`).
   - Many threads include XML/Python snippets and UI screenshots.
   - **Odoo Community Association (OCA)**
     https://odoo-community.org/

   - Explore OCA modules like `auth_oauth`, `base_import`, and `auditlog`.
   - Access community-maintained documentation for advanced administrative features.

Pro Tip: Always search before posting—most common administrative issues (e.g., "user can't see records") have already been solved.

3. **Structured Learning Paths for Odoo 16 Administrative Management**

   To build your skills systematically, follow these recommended paths—ideal for system administrators, IT managers, and compliance officers.

   Beginner Path: User & Access Setup

   (a) User and Company Creation
   – Set up internal users, link to companies, send invitations.

   (b) Security Groups and Menus
   – Assign users to predefined groups (Sales, HR, etc.).

   (c) Basic Data Import/Export
   – Use CSV templates to bulk-load contacts or users.

   Intermediate Path: Security & Governance

   (a) Record Rules and Data Isolation
   – Configure row-level visibility (e.g., by company or department).

   (b) External Authentication
   – Integrate LDAP, Azure AD, or Google SSO.

   (c) Multi-Company Administration
   – Manage data separation across legal entities.

   (d) Access Reviews and Cleanup
   – Identify and archive inactive users quarterly.

   Advanced Path: Compliance & Automation

   (a) Audit Logging (Enterprise)
   – Monitor user actions and generate compliance reports.

   (b) Custom Security Groups
   – Build fine-grained roles (e.g., "HR Data Steward").

   (c) Automated User Provisioning
   – Use HR app to auto-create users on employee hire.

   (d) Backup and Recovery Strategy
   – Schedule and test database restores.

4. **Free & Community-Driven Learning Resources**

5. **YouTube Tutorials (Community Creators)**
   Channels like *Odoo Mates*, *Thinkwell*, and *ERP School* offer practical walkthroughs.
   Search: "Odoo 16 user management", "Odoo record rules", "Odoo SSO setup"

6. **GitHub Repositories (OCA)**
   Explore open-source administrative modules:
   https://github.com/OCA/server-auth
   https://github.com/OCA/server-tools
   https://github.com/OCA/auditlog

7. **Reddit & LinkedIn Groups**

   - r/odoo on Reddit: https://www.reddit.com/r/odoo/
   - LinkedIn: Search for "Odoo Administrators" or "Odoo Security Professionals"

   Note: Always verify compatibility with Odoo 16, as administrative features and UIs evolve across versions.

12.3 Frequently Asked Questions (FAQs) and Troubleshooting Guide

This section covers the most common questions and issues encountered when managing users, access rights, data operations, and system configuration in Odoo (v16). Use this guide to quickly resolve errors, understand system behavior, and ensure secure, compliant administrative operations.

1. **User Management**

   Q1: A new user didn't receive the invitation email—what should I do?

   A:

   (a) Check if the email address was entered correctly in the user record.

   (b) Verify that Odoo's outgoing mail server is configured (`Settings → General Settings → Discuss → Test Email Setup`).

   (c) Manually resend the invitation: open the user record → click **Send Reset Password Instructions**.

   (d) If using SSO (e.g., LDAP), ensure "Invite User" is enabled—some SSO setups skip email invites.

   Q2: Why can't a user log in even after activation?

   A:

   (a) Confirm the user is **Active** (not archived) in `Settings → Users & Companies → Users`.

   (b) If using external authentication (LDAP/OAuth), verify the user exists in the identity provider.

(c) Check for IP or session restrictions (e.g., via system parameters or firewall rules).

2. **Access Rights & Permissions**

Q3: A user can't see records they should have access to—why?

A:

This is usually due to record rules or group misconfiguration:

(a) Verify the user is assigned to the correct security group(s) (`Access Rights` tab on user form).

(b) Check `Settings → Technical → Security → Record Rules` for domain filters that may restrict visibility (e.g., company-based rules).

(c) In multi-company setups, ensure the user is linked to the correct company—and that "Allow Multi-Company" is enabled if needed.

(d) Test by logging in as the user (use **Impersonate** in Developer Mode).

Q4: How do I give a user access to only one department's data?

A:

(a) Create a custom record rule on the relevant model (e.g., `hr.employee`, `res.partner`).

(b) Use a domain like `[('department_id.name', '=', 'Sales')]`.

(c) Assign the rule to a new security group, then add the user to that group.

(d) *Note:* Requires **Developer Mode** to configure.

3. **Data Import/Export**

Q5: My CSV import fails with "No value found for field..."—how do I fix it?

A:

(a) Download the official import template from the list view (click **Import** → **Download Template**).

(b) Ensure column headers exactly match Odoo field names (case-sensitive).

(c) For relational fields (e.g., Customer, Product), use the **name** or **External ID**—not internal database IDs.

(d) Required fields (e.g., email for users) must not be empty.

(e) Use **Test Import** before finalizing to catch errors early.

Q6: Why can't a user export certain records even though they're visible in the UI?

A:

(a) Odoo's export function respects the same access rules as the UI—but sometimes record rules behave differently in batch operations.

(b) Check if the user has **read** access to all fields being exported (via `ir.model.access`).

(c) In multi-company setups, ensure the export filter includes only the user's company.

(d) If using custom modules, verify export permissions are not overridden.

4. **Authentication & SSO**

Q7: LDAP login fails with "Wrong credentials"—but the password is correct.

A:

(a) Verify the LDAP server URL, port, and encryption (e.g., LDAPS on 636).

(b) Check the **LDAP Bind DN** and **Password**—this is the service account Odoo uses to query LDAP.

(c) Ensure the **LDAP Filter** matches your directory structure (e.g., `(uid=%(login)s)` for Unix, `(sAMAccountName=%(login)s)` for Active Directory).

(d) Test connectivity using an LDAP client (e.g., Apache Directory Studio).

Q8: Can I enable both local login and SSO?

A: Yes. Odoo supports mixed authentication:

(a) Users with an external ID (e.g., from LDAP) will be redirected to SSO.

(b) Users without an external ID can log in with a local password.

(c) Configure this in `Settings → Technical → Authentication`.

5. **Audit & Compliance (Enterprise)**

Q9: Why don't I see audit logs for user creation?

A:

(a) Audit logging is an **Odoo Enterprise** feature—ensure you're not using Community Edition.

(b) Go to `Settings → Technical → Logs → Audit Logs` and verify logs are enabled.

(c) By default, key models (`res.users`, `res.groups`) are tracked—custom models must be added manually.

Q10: How do I export audit logs for compliance review?

A:

(a) In `Audit Logs`, apply filters (e.g., date range, user, model).

(b) Click **Export** (top-right) and choose Excel or CSV.

(c) The export includes user, timestamp, IP address, and field changes.

Chapter 13

Comparison Between Enterprise and Community Editions

Feature	Community Edition	Enterprise Edition
User and Group Management	Fully supported: create users, assign groups, manage companies	Fully supported, with enhanced UI and bulk actions
Record Rules (Row-Level Security)	Fully supported: enforce data isolation via domain filters	Fully supported, with visual rule builder in Studio
Data Import/Export Engine	Supported: CSV/Excel import/export in all list views	Supported, with enhanced templates, validation, and error highlighting
External Authentication (SSO)	• LDAP: Supported (manual config via Developer Mode) • OAuth 2.0: Limited (requires custom code) • SAML: Not supported	• LDAP: Fully supported with UI configuration • OAuth 2.0: Pre-built connectors (Google, Azure AD, GitHub) • SAML: Fully supported (Okta, OneLogin, etc.)
Audit Logging	• No built-in audit trail • Basic login logs via `res.users.log` • Custom logging requires third-party modules (e.g., OCA `auditlog`)	• Full audit logging: tracks user actions, field changes, logins • Logs include user, timestamp, IP address, before/after values • Exportable for compliance (SOX, GDPR, ISO 27001)

Multi-Company Data Isolation	Supported via record rules and company fields	Supported, with visual validation and inter-company access controls
Role-Based Access Control (RBAC)	Fully supported via groups and ACLs	Fully supported, with Odoo Studio for no-code role customization
Developer Mode	Available: access technical settings, record rules, models	Available, with additional Enterprise-only debug tools
Custom Security Groups	Supported (via Developer Mode)	Supported, with drag-and-drop group builder in Studio
User Activity Monitoring	Limited to login timestamps	Real-time session tracking, last activity, and concurrent session alerts
Password Policy & 2FA	• Basic password reset • 2FA not supported	• Enforce password complexity • Built-in Two-Factor Authentication (TOTP, SMS, email)
Data Export Restrictions	Exports respect user permissions but no granular control	Fine-grained export policies (e.g., block exports for sensitive models)
Backup & Recovery	Manual database dumps required	Automated daily backups (Odoo.sh), one-click restore
Mobile App Access	Not optimized for admin tasks	Full access to user management and settings via Odoo mobile app
Priority Support	Community forums and GitHub issues only	Direct access to Odoo support team with SLAs

Table 13.1: Comparison of Odoo Administrative Features: Enterprise vs. Community Editions