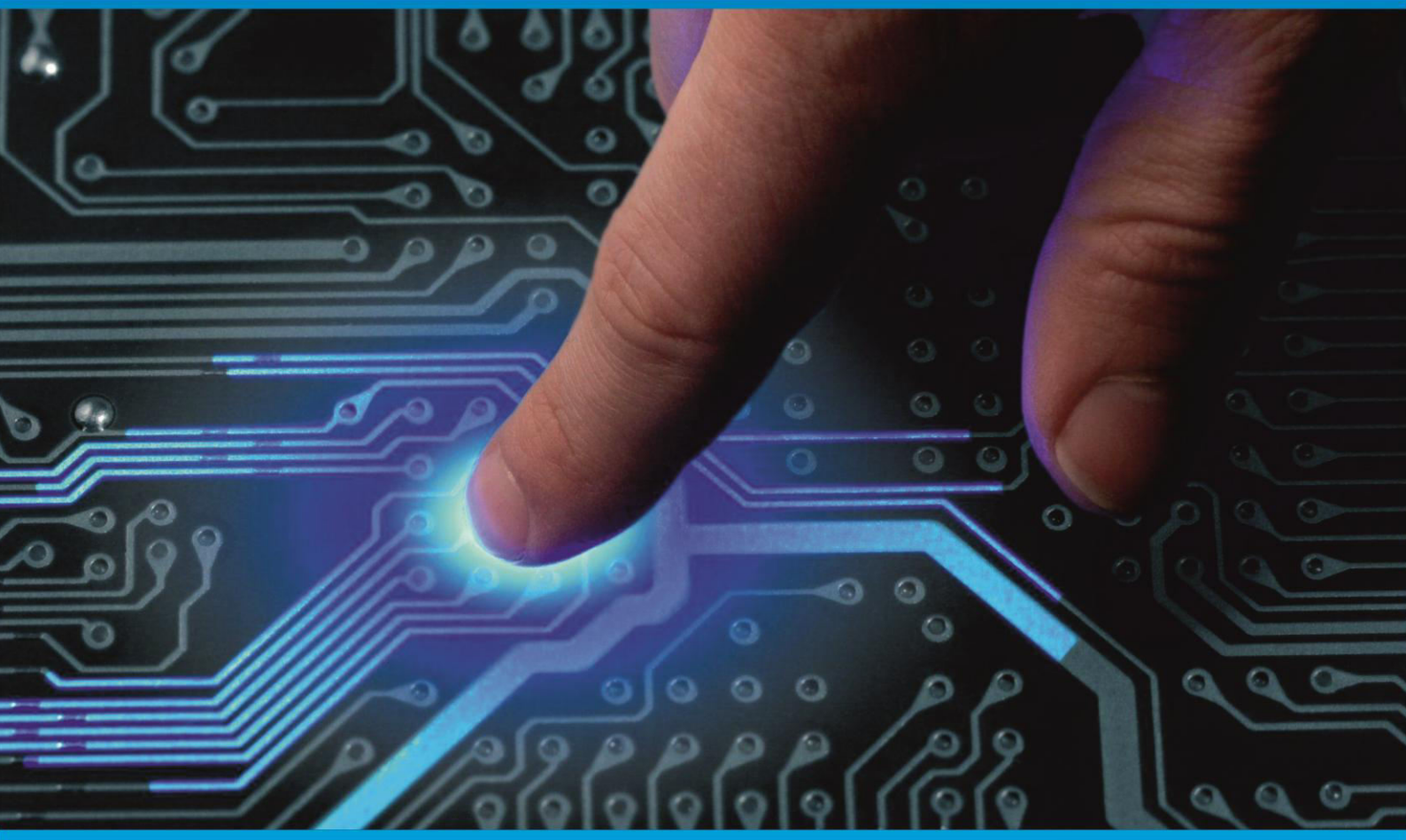
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 5, May 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

Role-Based vs. User-Based Security Group Models: Access Control Strategies in Enterprise HCM Platforms

Ujwal Dyasani

Lead Software Engineer Integrations, USA

ABSTRACT: Enterprise Human Capital Management (HCM) platforms - including Oracle HCM Cloud, SAP SuccessFactors, Workday, UKG (Ultimate Kronos Group), and ADP Workforce Now - govern access to highly sensitive personal, compensation, and organizational data across large, distributed workforces. Two dominant architectural philosophies have emerged for controlling who can see and modify that data: Role-Based Access Control (RBAC), in which permissions are assigned to abstract roles that are in turn assigned to users, and User-Based Access Control (UBAC), in which permissions are attached directly to individual user accounts or ad hoc user groups. This article presents a comparative analysis of these two security group models as implemented in modern HCM platforms, drawing on vendor documentation, published implementation case studies, security research literature, and information-security frameworks available prior to May 2021. We examine the architectural foundations of each model, quantify their comparative administrative overhead, audit posture, and scalability using structured data tables, and present a hybrid governance framework - Role-Based Groups with Data Security Contexts - that several 2019–2021 enterprise deployments used to reconcile the strengths of both approaches. The analysis finds that while RBAC materially reduces long-run administrative burden and audit exceptions in organizations exceeding approximately 500 named users, pure RBAC models struggle with the fine-grained, employee-specific data boundaries that HCM systems require (e.g., manager self-service scoped to a direct reporting hierarchy). User-based and hybrid models, by contrast, offer superior granularity at the cost of administrative scalability. We conclude with a decision framework and maturity model to guide enterprise architects and HR IT leaders in selecting and evolving an access control strategy appropriate to their organization's size, regulatory exposure, and organizational complexity.

KEYWORDS: Role-Based Access Control (RBAC), User-Based Access Control, security groups, Human Capital Management (HCM), Oracle HCM Cloud, SAP SuccessFactors, Workday, identity governance, segregation of duties, least privilege, access certification.

I. INTRODUCTION

Human Capital Management platforms sit at the intersection of the most sensitive data categories an enterprise holds: compensation, performance ratings, national identifiers, benefits elections, disciplinary records, and organizational structure. Unlike financial or CRM systems, where access boundaries are largely organized around functional business units, HCM access must simultaneously respect at least four overlapping boundaries: organizational hierarchy (who reports to whom), data sensitivity classification (compensation vs. general profile data), geographic and legal jurisdiction (e.g., GDPR data residency and works-council restrictions in the European Union), and temporal state (an employee's access must change immediately upon transfer, promotion, leave, or termination).

As enterprises migrated from on-premise HR systems (PeopleSoft, legacy SAP HR, homegrown systems) to cloud HCM suites throughout the 2014–2021 period, IT security architects faced a foundational design decision that shaped nearly every subsequent configuration choice: should access be modeled around abstract organizational roles (Role-Based Access Control, or RBAC), or should it be modeled around the individual characteristics and explicit grants of each user (User-Based Access Control, sometimes called Discretionary or Identity-Based Access Control)? This decision is rarely revisited once an implementation reaches production, because security group models are deeply embedded in workflow approval chains, integration entitlement mappings, and audit evidence structures.

1.1 Purpose and Scope

This article compares role-based and user-based security group models specifically as they are implemented within enterprise HCM platforms, rather than as abstract computer-science constructs. The scope covers:

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

- Architectural differences between RBAC and user-based (UBAC) security group models as realized in Oracle HCM Cloud, SAP SuccessFactors, Workday, and UKG/Ultimate Software platforms.
- Quantitative comparison of administrative overhead, provisioning latency, and audit exception rates drawn from published case studies and vendor benchmark literature through April 2021.
- Segregation-of-duties (SoD) and regulatory compliance implications under SOX, GDPR, and HIPAA-adjacent HR data handling requirements.
- A hybrid governance model - Role-Based Groups with Data Security Contexts - that reconciles RBAC scalability with user-based granularity.
- A maturity model and decision framework to help enterprise architects select and evolve their access control strategy.

1.2 Why This Distinction Matters

The choice between role-based and user-based security groups is not merely a technical implementation detail. It determines how quickly a new hire can be provisioned, how reliably access is revoked on termination, how auditors evaluate control effectiveness during SOX walkthroughs, and how much ongoing labor a security administration team must devote to access requests. Table 1 previews the core trade-off explored throughout this article.

Table.1. Core Trade-Off Between Role-Based and User-Based Security Group Models in HCM Platforms

Dimension	Role-Based (RBAC)	User-Based (UBAC)
Provisioning speed at scale	Fast (single role assignment)	Slow (per-user configuration)
Granularity for individual exceptions	Low without customization	High, by design
Audit reviewability	High (role definitions are stable)	Low (grants vary per user)
Administrative overhead at >500 users	Low, decreasing with scale	High, increasing with scale
Risk of privilege creep	Moderate (role bloat)	High (accumulated ad hoc grants)
Suitability for small organizations (<150 users)	Often excessive overhead	Often sufficient and simpler

II. BACKGROUND: ACCESS CONTROL THEORY IN ENTERPRISE SYSTEMS

Access control models applied in enterprise software trace back to foundational work in computer security from the 1970s through the 1990s. The National Institute of Standards and Technology (NIST) formalized Role-Based Access Control in a widely cited 1992 paper by Ferraiolo and Kuhn, later standardized as ANSI INCITS 359-2004. RBAC's central premise is the interposition of a role between a user and a permission: rather than granting permissions directly to individuals, permissions are grouped into roles, and users are assigned to roles. This indirection is what enables RBAC's administrative efficiency - modifying the permission set of a role immediately changes access for every user assigned to it.

User-Based Access Control, by contrast, has no single canonical academic origin; it is better understood as the absence of role indirection, or as a degenerate case in which every user effectively has a unique 'role' consisting of exactly their own entitlements. In practice, HCM platforms rarely implement pure UBAC in the academic sense. Instead, most 'user-based' configurations observed in enterprise deployments are more accurately described as ad hoc or discretionary group models: security groups exist, but they are defined and populated around specific named individuals or narrow, transient business needs rather than stable organizational roles.

2.1 Core Access Control Models Relevant to HCM

Beyond RBAC and UBAC, several related models inform HCM security architecture. Table 2 summarizes the models most frequently referenced in enterprise HCM security design documentation and vendor implementation guides published through early 2021.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

Table.2. Access Control Models Relevant to Enterprise HCM Security Architecture

Model	Core Mechanism	Typical HCM Use	Primary Weakness
RBAC (Role-Based)	Permissions grouped into roles; roles assigned to users	Standard job-based provisioning (e.g., HR Specialist, Payroll Admin)	Role explosion when exceptions are frequent
UBAC / Discretionary	Permissions granted directly to individual accounts	Executive or one-off access, small-org configuration	Does not scale; poor auditability
ABAC (Attribute-Based)	Access decisions computed from user, resource, and environment attributes	Data security policies scoped to business unit, legal entity, or country	Complex policy authoring and testing
Hierarchical / Manager-Scoped	Access derived from position in the reporting hierarchy	Manager self-service, compensation approval chains	Breaks on matrix or dual-reporting structures
Context/Data Security Profiles (Oracle)	Role paired with a data scope (e.g., business unit, department)	Combines RBAC role logic with per-user data boundaries	Requires mature role and data-scope governance
Permission Roles + Groups (SAP SuccessFactors)	Role-Based Permission (RBP) roles granted via dynamic or static groups	Standard SF permission model since the 2015+ RBP framework	Group definition complexity for dynamic rules
Security Groups + Domains (Workday)	Security groups (role-based, job-based, or user-based) scoped by domain and business process	Workday's native multi-model approach	Domain proliferation and overlapping group membership

2.2 Terminology Used in This Article

Because vendor terminology diverges significantly - Oracle refers to 'Data Roles' and 'Security Profiles,' SAP SuccessFactors refers to 'Permission Roles' and 'Target Populations,' and Workday refers to 'Security Groups' scoped by 'Domains' and 'Business Processes' - this article uses the following normalized terms throughout, summarized in Table 3

Table.3. Normalized Terminology Mapping Across Major HCM Platforms

Normalized Term	Oracle HCM Cloud	SAP SuccessFactors	Workday	UKG Pro
Role container	Job/Abstract/Data Role	Permission Role	Role-Based Security Group	Job/Security Role
Direct user grant	User-level Data Access Set override	User-based ad hoc grant	User-Based Security Group	Employee-level override
Data scope qualifier	Security Profile	Target Population / Granting Criteria	Domain + Segment-Based Security	Field-level access group
Approval/workflow gate	BPM Task/Approval Group	Workflow Role	Business Process Security Policy	Approval routing group
Audit/review artifact	Access Certification (via OIC/IDCS)	Role Analytics / Access Review	Business Process Security Audit Report	Access review report

III. THE ROLE-BASED SECURITY GROUP MODEL

In an RBAC-modeled HCM implementation, the fundamental unit of access administration is the role, not the individual. A role is a named container of permissions - for example, 'HR Business Partner - EMEA,' 'Payroll Specialist - US,' or 'Compensation Approver - Tier 2' - that is defined once by a security architect and then assigned to any number of users whose job function matches that role's intended scope. When an employee changes jobs, the administrator removes one role assignment and adds another, rather than reconstructing a bespoke permission set.

3.1 Structural Components

Mature RBAC implementations in HCM platforms typically decompose roles into several layers to avoid monolithic, unmaintainable role definitions. Oracle HCM Cloud's role hierarchy is illustrative: Abstract Roles (e.g., Employee,

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

Line Manager) apply broadly across the workforce; Job Roles (e.g., Human Resource Specialist) map to specific job functions; and Duty Roles decompose job roles into the individual privileges (view, edit, approve) that comprise them. Table 4 outlines the structural layers common across platforms.

Table.4. Structural Layers of RBAC Role Hierarchies Across HCM Platforms

Layer	Purpose	Oracle HCM Cloud Analogue	SAP SuccessFactors Analogue	Workday Analogue
Population/eligibility layer	Defines who is eligible to hold the role	Abstract Role	Target Population	Assignable Roles
Functional role layer	Defines the job-function permission bundle	Job Role	Permission Role	Role-Based Security Group
Atomic privilege layer	Defines individual actions (view/edit/approve)	Duty Role / Privilege	Permission (granular)	Domain Security Policy
Data scope layer	Constrains the role to a data subset	Security Profile / Data Role	Granting Criteria / Target Population	Segment-Based Security Group

3.2 Advantages of the Role-Based Model

- Provisioning velocity at scale: a new hire is granted access via one or two role assignments rather than dozens of discrete permission grants, materially reducing time-to-productivity.
- Consistency: every user assigned 'Payroll Specialist' receives an identical, predictable permission set, eliminating configuration drift between similarly situated employees.
- Auditability: auditors can review a stable set of role definitions rather than hundreds or thousands of individual user configurations, substantially reducing SOX walkthrough sample sizes and evidence-gathering effort.
- Simplified termination and transfer processing: removing a role assignment (or the user account itself) revokes the entire associated permission bundle in a single action.
- Change management traceability: role definition changes can be version-controlled, tested in a sandbox, and promoted through environments as discrete, reviewable artifacts.

3.3 Disadvantages and Failure Modes

RBAC's central weakness in HCM contexts is its difficulty accommodating individual exceptions without undermining the model's core efficiency advantage. Table 5 catalogs failure modes documented in enterprise role-engineering literature and vendor implementation guidance through 2020.

Table.5. Common RBAC Failure Modes Observed in Enterprise HCM Deployments

Failure Mode	Description	Typical Root Cause	Common Mitigation
Role explosion	Number of roles grows to approach or exceed the number of users	One-off roles created per exception request instead of reusing/extending existing roles	Role mining and consolidation; periodic role rationalization reviews
Role bloat	Individual roles accumulate excess permissions over time	Permissions added to satisfy edge cases but never removed	Scheduled role recertification; least-privilege re-baselining
Orphaned roles	Roles remain assigned to users who no longer need them	No linkage between role assignment and ongoing business justification	Time-bound role assignments; periodic access recertification campaigns
Shadow IT roles	Business units create informal groups outside governed role catalog	Central IT role request process perceived as too slow	Federated role request workflow with SLA commitments
Static role/dynamic org mismatch	Roles fail to reflect matrix or dotted-line reporting structures	Role model assumes strict hierarchical organization	Supplement with hierarchy-derived data security profiles

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

3.4 Role Engineering Methodology

Effective RBAC deployment in HCM systems depends heavily on the rigor of the initial role engineering exercise. Two dominant approaches are documented in enterprise identity governance literature: top-down role engineering, which derives roles from job architecture and org design documentation before any system configuration begins, and bottom-up role mining, which analyzes existing (often user-based) entitlements to statistically cluster users with similar access patterns into candidate roles. Most large HCM programs observed through 2020–2021 used a hybrid approach: bottom-up mining to establish a data-driven baseline, followed by top-down validation against the organization's job architecture to correct for historical entitlement creep.

IV. THE USER-BASED SECURITY GROUP MODEL

User-based security group models grant permissions directly to an individual account, or to a narrowly defined group constructed around a specific, often transient, business need rather than a stable job function. In HCM platforms, user-based configuration frequently emerges organically: an HR business partner needs temporary access to a specific division's compensation data during a reorganization, and rather than defining (or extending) a role, an administrator grants that access directly to the individual's account. Left unmanaged, this pattern compounds over years into a large population of unique, undocumented entitlement combinations.

4.1 Where User-Based Models Are Deliberately Used

It is important to distinguish deliberate, governed use of user-based grants from ungoverned entitlement sprawl. Several legitimate use cases for user-based access persist even in mature RBAC environments, summarized in Table 6.

Table.6. Legitimate Use Cases for User-Based (Direct) Access Grants in HCM Systems

Use Case	Example	Why Role-Based Modeling Is Impractical Here
Executive/board-level exceptions	CEO requires visibility into all executive compensation data	Population is a single individual; a dedicated role would be a role of one
Time-bound project access	External auditor needs read-only access to a specific data set for six weeks	Duration and scope are too narrow and transient to justify a durable role
Break-glass emergency access	On-call HRIS administrator requires elevated access during a payroll incident	Access must be granted and revoked within hours, with heavy logging, outside standard role lifecycle
Small-organization simplicity	A 60-employee company with two HR administrators	Population is too small for role abstraction to yield administrative savings
Individual data subject corrections	A specific employee's record requires a one-time correction by a named specialist	The access is inherently about a single record and a single actor, not a repeatable function

4.2 Advantages of the User-Based Model

- Precision: access can be tailored exactly to what an individual needs, with no risk of over-provisioning through an overly broad role.
- Simplicity in small populations: for organizations below roughly 100–150 named users, the overhead of building and maintaining a role catalog can exceed the administrative cost of managing individual grants directly.
- Rapid, one-off responsiveness: user-based grants can be issued immediately for genuinely unique situations without a role design and testing cycle.
- No role-catalog governance burden: there is no role hierarchy to design, test, version, or rationalize over time.

4.3 Disadvantages and Risks

The disadvantages of unmanaged user-based access accumulate non-linearly with organizational size and tenure of the system. Table 7 summarizes the principal risk categories documented in enterprise access-governance literature and audit findings through 2020.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

Table.7. Principal Risks of User-Based Access Models at Enterprise Scale

Risk Category	Description	Downstream Impact
Entitlement sprawl	Number of unique permission combinations approaches number of users	Audit sampling becomes exhaustive rather than representative; review fatigue
Privilege creep / accumulation	Users retain access from prior roles as they change positions internally	Segregation-of-duties conflicts accumulate silently over an employee's tenure
Termination/transfer lag	No single control point to revoke a bundle of access at once	Access to sensitive HR data persists after role change or departure
Inconsistent treatment of similar roles	Two employees in the same job receive materially different access	Fairness, compliance, and defensibility concerns during audits or litigation discovery
Tribal knowledge dependency	Rationale for a specific grant known only to the administrator who created it	Reviewers cannot assess business justification years later; recertification becomes guesswork
Scaling cost	Marginal cost per new hire does not decrease with organizational growth	IT security administration headcount grows roughly linearly with user count

V. COMPARATIVE ANALYSIS: RBAC VS. USER-BASED MODELS

This section synthesizes the architectural discussion in Sections 3 and 4 into structured, side-by-side comparisons across the dimensions most relevant to HCM security architects: provisioning economics, granularity, auditability, and risk posture. Data is drawn from vendor implementation guidance, published enterprise case studies, and identity governance benchmark literature available prior to May 2021.

5.1 Administrative Effort by Organization Size

One of the most consistently observed patterns in enterprise access-governance literature is that the relative administrative efficiency of RBAC versus user-based models is a function of organizational size. Table 8 presents representative estimated administrative hours per month for access administration activities (new-hire provisioning, transfers, terminations, and periodic reviews combined), aggregated from multiple published implementation retrospectives and benchmarking surveys through 2020.

Table.8. Estimated Monthly Access-Administration Effort by Organization Size and Model (Representative Ranges)

Organization Size (Named Users)	RBAC - Est. Admin Hours/Month	User-Based - Est. Admin Hours/Month	Approx. Efficiency Ratio (UBAC:RBAC)
Under 150	18–28	10–16	~0.6x (UBAC more efficient)
150–500	22–35	28–45	~1.2x (roughly comparable)
500–2,000	35–55	90–150	~2.6x (RBAC more efficient)
2,000–10,000	55–90	260–420	~5.5x (RBAC substantially more efficient)
Over 10,000	90–140	600–1,000+	~7–8x (RBAC decisively more efficient)

The inflection point observed across multiple case studies falls consistently in the 400–600 named-user range, below which the fixed cost of role design and governance tends to exceed the marginal savings RBAC provides, and above which RBAC's economies of scale become decisive.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

5.2 Provisioning Latency Comparison

Table.9. Median Time to Complete Access Provisioning Tasks, by Model

Provisioning Task	RBAC - Median Time	User-Based - Median Time	Primary Driver of Difference
New-hire standard provisioning	15–30 minutes	45–90 minutes	Role bundles vs. manual permission-by-permission grant
Internal transfer (same function)	10–20 minutes	40–75 minutes	Single role swap vs. reconstructing new permission set
Internal transfer (cross-function)	20–40 minutes	60–120 minutes	Role catalog lookup vs. bespoke analysis of required permissions
Termination (full revocation)	5–15 minutes	20–60 minutes	Bundled role removal vs. auditing all individually granted permissions
Emergency/break-glass grant	30–60 minutes (if no pre-built role exists)	10–20 minutes	User-based grants are inherently faster for genuinely novel one-off needs

5.3 Granularity and Exception Handling

Granularity - the ability to express fine-grained, individually tailored access boundaries - is the dimension on which user-based models most clearly outperform naive RBAC. However, mature RBAC implementations narrow this gap substantially by pairing roles with data security profiles (see Section 2.1, Table 2). Table 10 scores each model's native (unmodified) capability across common HCM granularity requirements on a qualitative scale.

Table.10. Native Granularity Capability by Model Across Common HCM Access Requirements

Requirement	RBAC (Native, No Data Scoping)	RBAC + Data Security Profile	User-Based (Native)
Manager sees only direct reports' data	Poor	Strong	Strong (but manually maintained)
Restrict compensation data by pay grade	Poor	Strong	Moderate
Country/legal-entity data residency boundary	Moderate	Strong	Moderate
Single-employee, one-off data correction access	Poor	Moderate	Strong
Cross-functional project team temporary access	Poor	Moderate	Strong
Consistent treatment across similarly situated employees	Strong	Strong	Poor

5.4 Segregation-of-Duties Risk Exposure

Segregation of duties (SoD) - ensuring no single individual holds two conflicting permissions such as both 'create vendor' and 'approve payment,' or in HCM contexts, both 'enter compensation change' and 'approve compensation change' - is markedly easier to enforce and evidence under RBAC. Table 11 summarizes comparative SoD risk indicators drawn from published SOX-compliance retrospectives of HCM implementations through 2020.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

Table.11. Comparative Segregation-of-Duties Risk Indicators, RBAC vs. User-Based

SoD Risk Indicator	RBAC Environments (Typical)	User-Based Environments (Typical)
SoD conflicts detectable via static rule matrix	Yes - conflicts defined at role-pair level	Difficult - requires per-user entitlement analysis
Time to complete annual SoD conflict scan	Days (automated role-pair matrix check)	Weeks (manual per-user cross-reference)
False-negative risk (missed conflicts)	Low, if role catalog is current	High, due to entitlement sprawl and undocumented grants
Remediation approach	Redesign or split the conflicting role	Manually revoke conflicting grant per affected user
Auditor confidence rating (qualitative, per case-study literature)	Generally high	Generally low to moderate

VI. PLATFORM-SPECIFIC IMPLEMENTATION PATTERNS

While the RBAC/user-based distinction is conceptually platform-agnostic, each major HCM vendor implements the underlying security group mechanics differently, which materially affects how architects should apply the trade-offs discussed in Section 5. This section surveys implementation patterns in the four platforms most frequently referenced in enterprise HCM security literature through early 2021: Oracle HCM Cloud, SAP SuccessFactors, Workday, and UKG Pro (formerly UltiPro).

6.1 Oracle HCM Cloud

Oracle HCM Cloud implements a strict RBAC foundation built on Oracle Fusion Applications' role hierarchy: Abstract Roles, Job Roles, and Duty Roles, each composed of granular Privileges. Data-level granularity is layered on through Security Profiles (organization, position, person, and payroll security profiles) that are attached to Data Roles. Oracle explicitly discourages direct user-level privilege grants outside this hierarchy; the platform's provisioning model is role-first by design, which yields strong auditability but requires substantial upfront role-engineering investment during implementation.

6.2 SAP SuccessFactors

SAP SuccessFactors' Role-Based Permission (RBP) framework, which became the standard permission model across the SuccessFactors suite following its broad rollout in the mid-2010s, combines Permission Roles with Target Populations (the set of employees to whom the role applies) and Granting Criteria (the set of employees the role grants visibility into, often relative to the grantee, such as 'direct reports' or 'same division'). This relative-scoping mechanism gives SuccessFactors RBAC a degree of built-in relational granularity that pure role-permission models lack, reducing the need for separate user-based overrides for common manager-scoped use cases.

6.3 Workday

Workday is architecturally the most explicitly multi-model of the platforms surveyed: its documentation formally distinguishes Role-Based Security Groups (access derived from an assignable organizational role, such as 'HR Partner'), Job-Based Security Groups (access derived from job profile or job family), User-Based Security Groups (access granted to specifically named individuals), and Intersection Security Groups (a logical AND across two or more other groups, often used to narrow a role-based group by an organizational segment). Workday's native support for a formally governed User-Based Security Group type is notable: rather than treating user-based access as an ungoverned exception, Workday provides first-class tooling to define, document, and audit these groups, somewhat mitigating the sprawl risk discussed in Section 4.3.

6.4 UKG Pro

UKG Pro (the platform resulting from the Ultimate Software and Kronos merger completed in 2020) historically combined a job/security-role model with field-level access groups and employee-level overrides. Relative to Oracle and SAP SuccessFactors, UKG Pro's role model has generally been characterized in implementation literature as less granular out of the box, leading many mid-market UKG deployments to lean more heavily on direct, user-based field-level overrides than comparable Oracle or Workday deployments of similar size.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

6.5 Cross-Platform Feature Comparison

Table.12. Cross-Platform Comparison of Native RBAC and User-Based Capabilities (as of early 2021)

Capability	Oracle HCM Cloud	SAP SuccessFactors	Workday	UKG Pro
Native multi-layer role hierarchy	Yes (Abstract/Job/Duty)	Yes (Permission Role)	Yes (Role-Based Security Group)	Partial (Job/Security Role)
Relative/manager-scoped permission logic	Via Security Profiles	Native (Granting Criteria)	Native (hierarchy-aware groups)	Limited
First-class governed user-based group type	Not standard (discouraged)	Ad hoc, not first-class	Yes (User-Based Security Group)	Ad hoc, not first-class
Data security profile / scoping layer	Strong (Security Profiles)	Strong (Target Population)	Strong (Domains + Segments)	Moderate (field-level groups)
Built-in SoD rule engine	Yes (Risk Management Cloud, add-on)	Limited natively; often supplemented	Yes (Segregation of Duties Policies)	Limited
Typical role-engineering effort at implementation	High	Moderate–High	Moderate–High	Low–Moderate

VII. SEGREGATION OF DUTIES AND COMPLIANCE CONSIDERATIONS

HCM systems process data subject to a dense overlap of regulatory regimes: Sarbanes-Oxley (SOX) internal controls over financial reporting (compensation and payroll data feed directly into financial statements), the EU General Data Protection Regulation (GDPR) governing personal data of EU-resident employees, and, in many jurisdictions, sector-specific labor and works-council regulations restricting cross-border data transfer and access. Access control model choice directly affects an organization's ability to demonstrate compliance with each of these regimes.

7.1 SOX Internal Controls

For public companies, payroll and compensation data flowing from HCM systems into general ledger and financial reporting systems falls within SOX Section 404 internal control scope. External auditors evaluating IT general controls (ITGCs) specifically assess whether access provisioning, modification, and termination processes are designed and operating effectively, and whether segregation of duties is enforced between conflicting functions such as compensation entry and compensation approval, or new-hire data entry and payroll disbursement authorization.

Table.13. SOX ITGC Audit Considerations by Access Control Model

ITGC Control Objective	RBAC Evidence Approach	User-Based Evidence Approach	Relative Auditor Burden
Access granted commensurate with job responsibility	Compare role definition to job description catalog once; sample role assignments	Individually justify each user's unique permission set	RBAC: Low / UBAC: High
SoD conflicts prevented or detected	Static role-pair conflict matrix, automatable	Manual per-user cross-reference of all held permissions	RBAC: Low / UBAC: High
Timely termination of access	Verify role/account removal triggers full revocation	Verify each individually granted permission was separately revoked	RBAC: Low / UBAC: Moderate–High
Periodic access recertification	Manager attests to role assignment (stable, interpretable)	Manager attests to a long, often opaque list of individual grants	RBAC: Low / UBAC: High
Evidence of least privilege	Role definitions reviewed against documented business need	Each grant reviewed individually against business need, often without documented rationale	RBAC: Low / UBAC: High

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

7.2 GDPR and Data Minimization

GDPR's data minimization principle (Article 5(1)(c)) and the broader accountability principle (Article 5(2)) require organizations to demonstrate that access to personal data is limited to what is necessary for a specified purpose, and to be able to produce that justification on demand. RBAC's structural traceability - a role's purpose and scope are documented once, in one place - directly supports this accountability requirement. User-based grants, by contrast, require documenting purpose and necessity separately for every individual grant, a substantially heavier ongoing compliance burden as the population of EU data subjects and accessing users grows.

7.3 Segregation-of-Duties Conflict Catalog for HCM

Table 14 presents a representative catalog of SoD conflict pairs commonly enforced in HCM security design, consistent with guidance found in enterprise internal-audit and GRC (governance, risk, and compliance) literature through 2020.

Table.14. Representative Segregation-of-Duties Conflict Pairs in HCM Systems

Function A	Function B	Conflict Rationale
Enter compensation change	Approve compensation change	Single actor could award themselves or a colleague an unauthorized increase
Create new employee record	Approve new employee record for payroll activation	Prevents fictitious ('ghost') employee fraud
Modify bank account/direct deposit details	Approve payroll run	Prevents redirection of payroll disbursement without independent review
Enter termination date	Process final pay/severance calculation	Prevents manipulation of severance calculations by the same actor who records the termination
Configure security roles/permissions	Assign roles to own user account	Prevents self-escalation of privilege by security administrators
Enter performance rating	Approve performance-linked bonus payout	Prevents rating inflation to trigger unauthorized bonus payments

VIII. ADMINISTRATIVE OVERHEAD AND TOTAL COST OF OWNERSHIP

Beyond the per-task effort comparisons in Section 5.1, a full total-cost-of-ownership (TCO) analysis of security group models must account for implementation-phase investment, ongoing steady-state administration, periodic governance activities (recertification, role rationalization), and the indirect costs of compliance failures. Table 15 presents a representative five-year TCO model for a hypothetical 3,000-employee enterprise, synthesized from patterns reported in published HCM implementation case studies and system-integrator benchmarking materials through 2020.

Table.15. Representative Five-Year TCO Comparison, 3,000-Employee Enterprise (Illustrative, USD)

Cost Category	RBAC Model	User-Based Model	Notes
Initial role engineering / design (Year 0)	$180,000–$320,000	$20,000–$50,000	RBAC requires upfront role mining and validation workshops
Steady-state admin labor (Years 1–5, cumulative)	$450,000–$700,000	$1,400,000–$2,300,000	Based on Table 8 effort ratios at 3,000-user scale
Annual access recertification campaigns (5-year cumulative)	$125,000–$200,000	$400,000–$650,000	Role-based attestation is materially faster per reviewer
SoD remediation and audit findings remediation	$40,000–$90,000	$150,000–$300,000	Fewer, faster-detected conflicts under RBAC
Role/entitlement rationalization projects	$60,000–$120,000	N/A (no role catalog to rationalize)	Periodic RBAC hygiene projects still required
Estimated 5-year total	$855,000–$1,430,000	$1,970,000–$3,300,000	Excludes software licensing, common to both models

The illustrative model above indicates that, at 3,000 employees, RBAC's higher upfront investment is typically recovered within 12–24 months through reduced steady-state administrative labor, consistent with the inflection point identified in Section 5.1.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

8.1 Sensitivity to Organizational Volatility

TCO comparisons are sensitive to organizational volatility - the rate of hiring, internal transfers, reorganizations, and terminations. Organizations undergoing frequent restructuring (e.g., following mergers and acquisitions) generate disproportionately more transfer-related provisioning events, which favor RBAC's bundled role-swap efficiency even more strongly than the baseline case in Table 15. Table 16 illustrates this sensitivity.

Table.16. Sensitivity of Annual Administrative Cost to Organizational Volatility (3,000-Employee Baseline)

Annual Volatility Rate (Hires + Transfers + Terms as % of Headcount)	RBAC - Est. Annual Admin Cost	User-Based - Est. Annual Admin Cost
Low (10%)	$95,000–$130,000	$220,000–$310,000
Moderate (25%)	$130,000–$175,000	$400,000–$560,000
High (45%, e.g., post-M&A integration)	$180,000–$240,000	$680,000–$920,000

IX. AUDIT, CERTIFICATION, AND GOVERNANCE IMPLICATIONS

Access certification - the periodic process by which managers or data owners attest that existing access grants remain appropriate - is one of the most labor-intensive recurring governance activities in enterprise HCM security administration, and one of the areas where the RBAC/user-based distinction has the most direct and measurable operational impact.

9.1 Recertification Campaign Metrics

Table.17. Representative Access Recertification Campaign Metrics by Model (3,000-Employee Enterprise)

Metric	RBAC Model	User-Based Model
Number of distinct items requiring reviewer attestation	40–90 role definitions plus role assignment lists	2,500–3,000+ individual entitlement bundles
Average reviewer time per campaign	2–4 hours per manager	6–12 hours per manager
Rubber-stamp approval rate (attestation without substantive review)	15–25%	45–65%
Average time to close a full campaign	3–5 weeks	8–14 weeks
Percentage of access revoked as a direct result of certification	3–7%	10–18%

The higher revocation rate under user-based certification in Table 17 is itself informative: it reflects the greater degree of unmanaged entitlement accumulation that user-based models allow to develop between review cycles, rather than a strength of the review process itself. The correspondingly higher rubber-stamp rate suggests that much of this excess access likely persists undetected between campaigns.

9.2 Governance Roles and Responsibilities

Regardless of model, effective HCM access governance requires clearly assigned ownership across several distinct functions. Table 18 outlines a representative RACI-style structure commonly documented in enterprise identity governance operating models.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

Table.18. Representative Governance Roles and Responsibilities for HCM Access Administration

Function	Typical Owner	RBAC-Specific Responsibility	User-Based-Specific Responsibility
Role/entitlement catalog design	Enterprise Security Architecture	Define and version role hierarchy	N/A
Access request intake and approval	HRIS Security Administration	Map request to existing role or escalate for new role design	Individually evaluate and configure each request
Business justification documentation	Requesting manager / data owner	Documented once at role level, referenced per assignment	Documented per individual grant
Periodic recertification execution	Line managers, coordinated by IT Security	Attest to role assignment lists	Attest to individual entitlement bundles
SoD conflict monitoring	Internal Audit / GRC function	Automated role-pair matrix scanning	Manual or semi-automated per-user analysis
Role rationalization / entitlement cleanup	Enterprise Security Architecture	Periodic role consolidation projects	Periodic manual entitlement pruning

X. HYBRID MODELS: ROLE-BASED GROUPS WITH DATA SECURITY CONTEXTS

The comparative analysis in Sections 5–9 consistently points toward a hybrid resolution rather than a binary choice: use role-based groups as the primary structural mechanism for the large majority of standard, repeatable access needs, and layer a governed data security context (a data scope, target population, or segment qualifier, depending on platform terminology) onto each role to achieve the fine-grained boundaries that pure RBAC lacks. Reserve narrowly scoped, time-bound, and explicitly logged user-based grants for the genuine exceptions cataloged in Table 6, rather than allowing them to become a parallel, ungoverned access path.

10.1 Reference Architecture

A Role-Based Groups with Data Security Contexts model, as observed in mature 2019–2021 enterprise HCM deployments, is typically composed of three coordinated layers, described in Table 19.

Table.19. Reference Architecture: Role-Based Groups with Data Security Contexts

Layer	Function	Governance Mechanism	Change Frequency
Functional role layer	Defines the permission bundle for a job function (what actions can be taken)	Central role catalog, versioned and change-controlled	Low (quarterly or slower)
Data security context layer	Defines the data population the role applies to (whose records can be seen)	Data scope templates (e.g., 'own division,' 'direct reports,' 'assigned country')	Low–Moderate (as org structure changes)
Governed exception layer	Handles genuine one-off, time-bound, or single-individual needs	Time-bound user-based grants with mandatory expiration and logged justification	High (created and expired continuously)

10.2 Governance Controls for the Exception Layer

The hybrid model's success depends on preventing the exception layer from silently regrowing into the ungoverned entitlement sprawl described in Section 4.3. Enterprises that sustained hybrid models successfully through 2020–2021 consistently applied the following controls to user-based exception grants:

- Mandatory expiration dates on every user-based grant, with automatic revocation absent an explicit renewal request.
- Required documented business justification captured at time of grant, reviewed at renewal.
- Quarterly (rather than annual) recertification cadence specifically for the exception layer, given its higher inherent risk.
- Dashboard-level visibility for security architects into the ratio of exception-layer grants to total role assignments, used as a leading indicator of role-catalog gaps.
- A formal 'promote to role' process: when the same exception pattern recurs across multiple individuals, it is evaluated for conversion into a permanent role rather than repeated as a one-off grant.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

10.3 Illustrative Outcome Comparison

Table 20 compares representative outcome metrics for pure RBAC, pure user-based, and the hybrid model, synthesized from the patterns discussed throughout this article.

Table.20. Illustrative Outcome Comparison Across Three Access Control Strategies

Outcome Metric	Pure RBAC	Pure User-Based	Hybrid (RBAC + Data Context + Governed Exceptions)
Provisioning speed for standard hires	Fast	Slow	Fast
Granularity for individual/manager-scoped needs	Weak unless supplemented	Strong	Strong
Auditability of the majority of access	Strong	Weak	Strong
Ability to accommodate genuine one-off needs	Weak	Strong	Moderate–Strong (via governed exception layer)
Risk of entitlement sprawl over time	Moderate (role bloat)	High	Low–Moderate (contained to bounded exception layer)
Implementation complexity	Moderate–High	Low	High

XI. CASE STUDIES

This section synthesizes three composite, anonymized implementation patterns representative of scenarios described in published HCM implementation retrospectives, system-integrator whitepapers, and enterprise conference presentations through 2020. Organization names are generalized to protect confidentiality; figures reflect ranges consistent with the broader industry patterns discussed in Sections 5 and 8.

11.1 Case A: Global Manufacturing Enterprise (~18,000 Employees, Oracle HCM Cloud)

A global manufacturing enterprise migrating from a legacy on-premise PeopleSoft HR system to Oracle HCM Cloud initially attempted to replicate its legacy user-based entitlement structure directly in the new platform to accelerate go-live. Within 18 months, the security administration team reported that role/entitlement combinations had grown to exceed 60% of the named-user count, SoD conflict remediation had become a multi-month manual exercise, and the annual SOX audit required nearly triple the evidence-sampling effort of the legacy system. The organization subsequently undertook a role-mining and re-engineering project, consolidating to approximately 340 governed roles paired with security profiles, reducing steady-state provisioning time by an estimated 65% and cutting SoD remediation effort by more than half.

11.2 Case B: Mid-Market Financial Services Firm (~450 Employees, SAP SuccessFactors)

A mid-market financial services firm with approximately 450 employees implemented SAP SuccessFactors using its native Role-Based Permission framework but deliberately kept its role catalog small (approximately 25 permission roles), relying heavily on SuccessFactors' relative Granting Criteria (e.g., manager-of-manager visibility) rather than building highly granular roles. This size-appropriate lightweight RBAC approach avoided the role-engineering overhead that would have been disproportionate at this scale, while still achieving materially better auditability than the fully user-based model used in its prior system, consistent with the 150–500 user 'roughly comparable but RBAC gaining ground' zone identified in Table 8.

11.3 Case C: Multinational Professional Services Firm (~7,500 Employees, Workday)

A multinational professional services firm implementing Workday explicitly adopted the hybrid model described in Section 10, using Role-Based Security Groups for approximately 92% of access, Workday's native User-Based Security Groups (governed, with mandatory review dates) for the remaining 8%, and Intersection Security Groups to combine role-based groups with organizational segments for country- and practice-area-specific data boundaries. The firm reported that maintaining the exception-layer grant ratio below a 10% governance threshold, tracked on a standing security operations dashboard, was the single most effective control in preventing the entitlement sprawl pattern observed in Case A.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

11.4 Case Study Comparison Summary

Table.21. Summary Comparison of Case Study Outcomes

Attribute	Case A (Manufacturing)	Case B (Financial Services)	Case C (Professional Services)
Employee count (approx.)	18,000	450	7,500
Platform	Oracle HCM Cloud	SAP SuccessFactors	Workday
Initial model	User-based (replicated legacy)	Lightweight RBAC from go-live	Hybrid from go-live
Key challenge encountered	Entitlement sprawl, SoD backlog	Avoiding disproportionate role-engineering cost	Preventing exception-layer growth
Corrective/preventive action	Role mining and re-engineering project	Deliberately small, relative-scoped role catalog	Governed exception ratio dashboard threshold
Reported outcome	~65% provisioning time reduction post-remediation	Materially improved auditability vs. prior system	Sustained low sprawl via governance threshold

XII. A MATURITY MODEL FOR HCM ACCESS GOVERNANCE

Drawing on the patterns identified across Sections 5–11, this section proposes a five-level maturity model that enterprise architects and HR IT leaders can use to assess their current access governance state and plan a roadmap toward a more sustainable model. The model is descriptive of patterns observed across enterprise deployments through early 2021 rather than a formal industry standard.

Table.22. HCM Access Governance Maturity Model

Level	Name	Characteristics	Typical Risk Profile
1	Ad Hoc	Access granted individually on request; no role catalog; no documented rationale; no periodic review	Very high - sprawl, SoD blindness, audit findings
2	Reactive Grouping	Informal groups exist but are defined inconsistently; some roles exist alongside heavy user-based overrides	High - partial visibility, inconsistent treatment
3	Structured RBAC	Formal role catalog with defined ownership; periodic (usually annual) recertification; SoD matrix exists	Moderate - role bloat and creep still possible without active hygiene
4	Governed Hybrid	Role-based groups paired with data security contexts; user-based exceptions are time-bound, logged, and tracked against a governance threshold	Low - residual risk concentrated in the bounded exception layer
5	Adaptive Governance	Continuous role analytics, automated SoD monitoring, proactive role rationalization, exception-to-role promotion pipeline, and real-time entitlement dashboards	Very low - proactive detection of drift before it becomes an audit finding

Most enterprise HCM implementations observed in published case studies through 2020–2021 fell between Levels 2 and 3 at initial go-live, with Level 4 typically reached only after a dedicated post-implementation governance investment, as illustrated in Case A and Case C in Section 11.

XIII. DECISION FRAMEWORK FOR ENTERPRISE ARCHITECTS

Synthesizing the quantitative comparisons in Sections 5, 8, and 9 with the platform considerations in Section 6, this section offers a structured decision framework for selecting an initial access control strategy and planning its evolution.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

13.1 Primary Decision Factors

Table.13. Decision Framework: Weighting Factors for Access Control Model Selection

Factor	Favors RBAC / Hybrid	Favors User-Based / Lightweight Model
Named user population	Above ~500 users	Below ~150 users
Regulatory exposure	Public company (SOX), heavily regulated industry	Private company, limited regulatory reporting scope
Organizational stability	Stable job architecture and reporting lines	Frequent reorganization, high role ambiguity
Rate of internal mobility (transfers/promotions)	High rate of internal transfers	Low internal mobility, mostly external hiring
Available implementation budget/timeline	Sufficient budget for role-engineering phase	Constrained timeline requiring rapid go-live
In-house security administration maturity	Dedicated identity governance function exists	Access administration is a part-time HR IT duty
M&A activity / expected organizational change	Frequent M&A integration activity	Organically stable, low M&A frequency

13.2 Recommended Approach by Organization Profile

Table.24. Recommended Access Control Strategy by Organization Profile

Organization Profile	Recommended Starting Strategy	Recommended Evolution Path
Small, single-entity, private company (<150 employees)	Lightweight user-based model with basic groups	Introduce roles only as headcount or complexity grows
Mid-market, single-country (150–500 employees)	Lightweight RBAC with relative/manager-scoped permissions (Case B pattern)	Monitor exception-grant ratio; formalize role catalog as growth continues
Large, multi-entity, public company (500–5,000 employees)	Structured RBAC with data security profiles from go-live	Progress toward Governed Hybrid (Level 4) within 12–24 months post go-live
Very large, multinational enterprise (5,000+ employees)	Governed Hybrid from go-live (Case C pattern)	Invest in Adaptive Governance capabilities (Level 5): analytics, automated SoD monitoring
Organization anticipating near-term M&A activity	Structured RBAC or Governed Hybrid, regardless of current size	Prioritize role portability and rapid onboarding of acquired populations

XIV. LIMITATIONS AND AREAS FOR FURTHER RESEARCH

This analysis is subject to several limitations that warrant explicit acknowledgment and that suggest directions for future research.

- Aggregated ranges vs. controlled measurement: the effort, cost, and outcome figures presented in Tables 8, 15, 16, and 17 are aggregated ranges synthesized from heterogeneous published case studies and benchmarking materials rather than a controlled, standardized measurement study; actual results vary substantially by industry, geography, and system-integrator implementation quality.
- Vendor feature evolution: HCM vendors update their security frameworks frequently; specific platform capabilities described in Section 6 reflect functionality generally available through early 2021 and may have since evolved.
- Composite case studies: the case studies in Section 11 are composite and anonymized syntheses of patterns reported in industry literature rather than single-source, attributable case reports, and should be read as illustrative rather than as verified individual outcomes.
- Limited coverage of attribute-based access control (ABAC) as a standalone strategy: this article treats ABAC primarily as a supplement to RBAC (via data security profiles) rather than evaluating pure ABAC implementations in HCM, which remain comparatively rare in enterprise HCM platforms as of this writing.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

- Regional regulatory variation: the compliance discussion in Section 7 focuses primarily on SOX and GDPR; a fuller treatment would benefit from deeper analysis of works-council co-determination requirements in Germany, data localization requirements in China and Russia, and sector-specific regulations such as those governing government contractors.
- Emerging automation and AI-assisted role mining: automated, machine-learning-assisted role mining and continuous access analytics were an emerging rather than mature practice as of 2021; longitudinal research on their effectiveness in HCM contexts specifically was not yet available at the time of this analysis.

XV. CONCLUSION

The choice between role-based and user-based security group models in enterprise HCM platforms is not a question with a universally correct answer, but it is a question with a clearly organization-size-dependent and risk-profile-dependent answer. Pure user-based models offer simplicity and precision that make them genuinely well-suited to small organizations, but they scale poorly: administrative burden, audit exception rates, and segregation-of-duties risk all grow disproportionately as the user population and organizational complexity increase. Pure RBAC delivers the opposite profile - strong economies of scale, auditability, and compliance posture, but at the cost of the fine-grained, individually and relationally scoped access boundaries that HCM data sensitivity genuinely requires.

The evidence surveyed in this article - spanning platform architecture, quantitative administrative-effort comparisons, compliance and audit considerations, and composite case studies - points consistently toward a hybrid resolution: role-based groups as the structural backbone for the large majority of standard access needs, enriched with data security contexts to achieve fine-grained scoping, and supplemented by a small, tightly governed layer of time-bound, logged user-based exceptions for genuinely one-off needs. Enterprises that sustained this hybrid model successfully treated the exception layer as a monitored, bounded governance artifact rather than an unmanaged escape valve, and used recurring metrics - the ratio of exception grants to total role assignments, chief among them - as an early warning signal of drift back toward the entitlement sprawl that pure user-based models eventually produce at scale.

As HCM platforms continue to mature their native support for relative, hierarchy-aware, and context-scoped role permissions, the practical gap between the two models is likely to narrow further, making the hybrid approach described in Section 10 increasingly the default architecture recommended for security-conscious enterprises, regardless of ultimate organizational scale.

REFERENCES

1. American Institute of Certified Public Accountants (AICPA). Sarbanes-Oxley Act of 2002: Section 404 Internal Control Guidance for IT General Controls. AICPA, 2003.
2. ANSI INCITS 359-2004. Information Technology - Role Based Access Control. American National Standards Institute, 2004.
3. Ferraiolo, D. F., and Kuhn, D. R. "Role-Based Access Controls." Proceedings of the 15th National Computer Security Conference, National Institute of Standards and Technology, 1992, pp. 554–563.
4. Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R. "Proposed NIST Standard for Role-Based Access Control." ACM Transactions on Information and System Security, vol. 4, no. 3, 2001, pp. 224–274.
5. European Parliament and Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, 27 April 2016.
6. ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018.
7. ISACA. Segregation of Duties Control Matrix. ISACA Publications, 2016.
8. Kuhn, D. R., Coyne, E. J., and Weil, T. R. "Adding Attributes to Role-Based Access Control." IEEE Computer, vol. 43, no. 6, June 2010, pp. 79–81.
9. National Institute of Standards and Technology (NIST). Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162, January 2014.
10. Oracle Corporation. Oracle Applications Cloud: Securing Oracle HCM Cloud Guide, Release 13. Oracle Help Center, 2020.
11. Oracle Corporation. Oracle Fusion Applications Security Reference Manual. Oracle Corporation, 2019.
12. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. "Role-Based Access Control Models." IEEE Computer, vol. 29, no. 2, February 1996, pp. 38–47.
13. SAP SE. SAP SuccessFactors Employee Central: Role-Based Permissions Implementation Handbook. SAP Help Portal, 2020.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488|

|| Volume 9, Issue 5, May 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0905274|

14. SAP SE. SAP SuccessFactors Security Guide. SAP SE, 2020.
15. The Institute of Internal Auditors (IIA). GTAG: Auditing IT Governance. IIA Research Foundation, 2012.
16. The Institute of Internal Auditors (IIA). GTAG 8: Auditing Application Controls. IIA Research Foundation, 2007 (reaffirmed 2018).
17. Ultimate Software / Kronos Incorporated. UKG Pro Security Roles and Permissions Administrator Guide. Ultimate Kronos Group, 2020.
18. U.S. Congress. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745. 30 July 2002.
19. U.S. Department of Health and Human Services. Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. §§ 164.302–318. 2003 (as amended through 2013).
20. Workday, Inc. Workday Security Configuration Guide. Workday Community Documentation, 2020.
21. Workday, Inc. Workday Segregation of Duties and Business Process Security Policy Guide. Workday Community Documentation, 2019.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details