

**ENHANCING DATA PROTECTION AND COMPLIANCE IN HUMAN CAPITAL  
MANAGEMENT SYSTEMS THROUGH INTEGRATED ACCESS REQUEST AND  
APPROVAL WORKFLOWS**

*Shweta Pandey*  
*shweta1780@gmail.com*

*Sumit Pandey*  
*sumpandey@gmail.com*

---

*Abstract*

*Human Capital Management (HCM) systems are critical repositories of personal and confidential workforce data, necessitating stringent employee data protection to comply with privacy regulations. Contemporary cloud-based HCM solutions offer mechanisms such as roles and security groups, enabling organizations to enforce robust security policies and ensure appropriate access controls for diverse user groups within the company. Despite these capabilities, the request and approval process for accessing various roles and security groups often occurs outside the HCM system, limiting the Human Resources (HR) team's oversight of these requests and their subsequent approvals. Integrating the access request and approval processes within the HCM system itself can enhance control, allowing HR teams and system administrators to more effectively track, report, and audit security modifications. This article delves into the architecture of security groups, the design of request business process workflows, the utilization of questionnaires, and the integration methodologies necessary to establish a comprehensive framework for managing access requests and approvals within an HCM system. Furthermore, it examines specific tools and functionalities provided by Workday to support this integration, thereby enhancing the overall security and compliance posture of HCM systems.*

*Keywords: Human Capital Management, Data Protection, Request Business Process, Questionnaire, JIRA, Service Now, Zendesk.*

**I. INTRODUCTION**

Security is a critical consideration for Human Capital Management (HCM) systems, as they contain sensitive and Personally Identifiable Information (PII) of employees [1,10,14]. This responsibility places significant pressure on HR departments to act as vigilant custodians of their employees' data [13]. HR departments manage some of a company's most valuable information, including Social Security numbers and other personal details, which must be diligently protected [4,13,14]. A breach in employee data security can result in reputational damage, loss of confidentiality, exposure of personal information, and substantial penalties [3,11].

To enhance HR data security, organizations must develop policies dictating who can access data [1,2,10,11] and who is authorized to approve access requests to the HCM system. Identifying key stakeholders and individuals who require regular data access is crucial [2,10,11,13,14], along with establishing a request and approval framework [12] to manage access to systems hosting personal and confidential employee data. A centralized process for requesting HCM access is essential [14], and it is equally important to route these

approvals to the appropriate owners or administrators [12] of functional areas such as Compensation, Core HR, Benefits, Absence, Talent & Performance, Recruiting, and Payroll.

In many organizations, access requests are initiated, approved, and tracked via email, which can compromise HCM system data security. Some organizations use ticketing tools like Service Now, JIRA, or Zendesk to track access requests and approvals. However, these methods often require the HCM system administration team to fulfil access requests, necessitating reconciliation processes to ensure alignment between approved and granted access [14].

An integrated and automated solution for access requests, approvals, and fulfilment within the HCM system would significantly enhance the security access request process. Implementing such a solution within HCM systems like Workday can eliminate manual errors, provide the HR team with better visibility, and facilitate easy reporting for audits and reconciliation [14].

## **II. PROBLEM STATEMENT**

Employees' personal information is among the most valuable data within a company, requiring HR to collaborate with the technology team to safeguard it through the implementation of stringent security policies and a robust request and approval process. HCM systems house highly sensitive information, including details about employees, payroll, and medical records [3]. Any breach or identity theft can impact not only the affected employee but the entire organization [3]. Whether facing external or internal threats, maintaining data integrity is paramount for any organization [3].

Internal threats, such as granting data access beyond what is necessary for an employee's role, can be as dangerous as external threats. Therefore, it is crucial for organizations to have a robust access request and approval system in place to prevent any lapses that could negatively impact the workplace. Many organizations currently track access request approvals outside the HCM system, using emails, and requests are manually fulfilled by HCM security administrators. However, relying on an email-based review and approval process introduces significant risks and can seriously harm the organization [6]. While email is an effective communication tool, it lacks the necessary features to maintain a smooth and secure review and approval process [6]. Issues with email-based tracking include security vulnerabilities, lack of an audit trail, version control challenges, quality assurance concerns, and the potential for human error [6]. Additionally, using external ticketing systems for tracking requests and approvals necessitates manual security entitlements, custom integration between the HCM and ticketing systems for reconciliation, and limited visibility for the HR team.

A custom solution leveraging Workday's request framework, business process workflows, questionnaires, studio integration, and extensive array of SOAP and REST-based web service APIs can enable organizations to create an automated solution for requesting, approving, and provisioning security groups within the HCM system. This solution would allow organizations to manage everything within the HCM system, providing better visibility for the HR team and facilitating easy reporting.

## **III. SOLUTION**

### **3.1 Questionnaire, Request Type, & Request Business Process**

Workday facilitates the creation and modification of questionnaires to collect information during business processes [8]. This functionality is streamlined through a single interface, allowing organizations to easily

create, edit, and duplicate questionnaires and questions [8]. Organizations can design questionnaires with various question types, such as date, numeric, and multiple-choice, with branching logic to gather comprehensive follow-up information [8]. These questionnaires can be configured as access request forms for the HCM system. Administrators can designate the 'Questionnaire Type' as "Request Initiation" and set 'Allowed on Business Processes' to "Request," thereby linking the questionnaire to a Request Type for use within the Request Business Process [7]. For instance, a questionnaire titled 'Access Provisioning Request' can be created with the following questions to form an access request:

- Access Request Type
- Security Role Required
- Justification

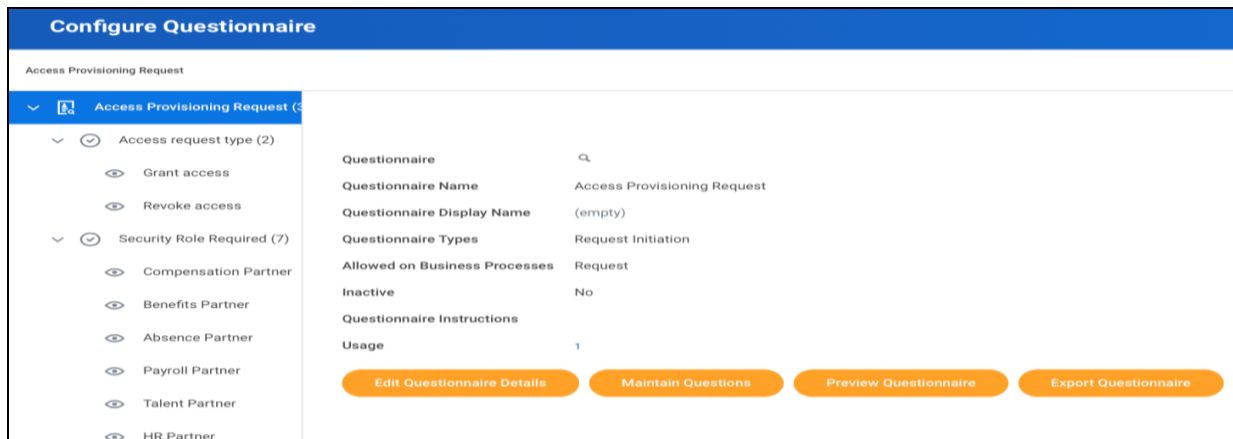


Fig 1: Configuration page of the Questionnaire

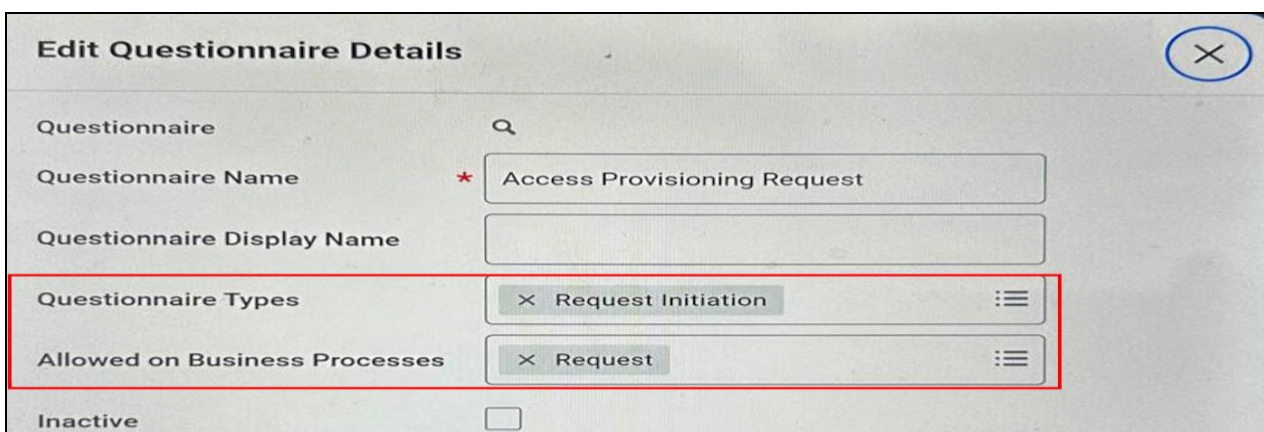
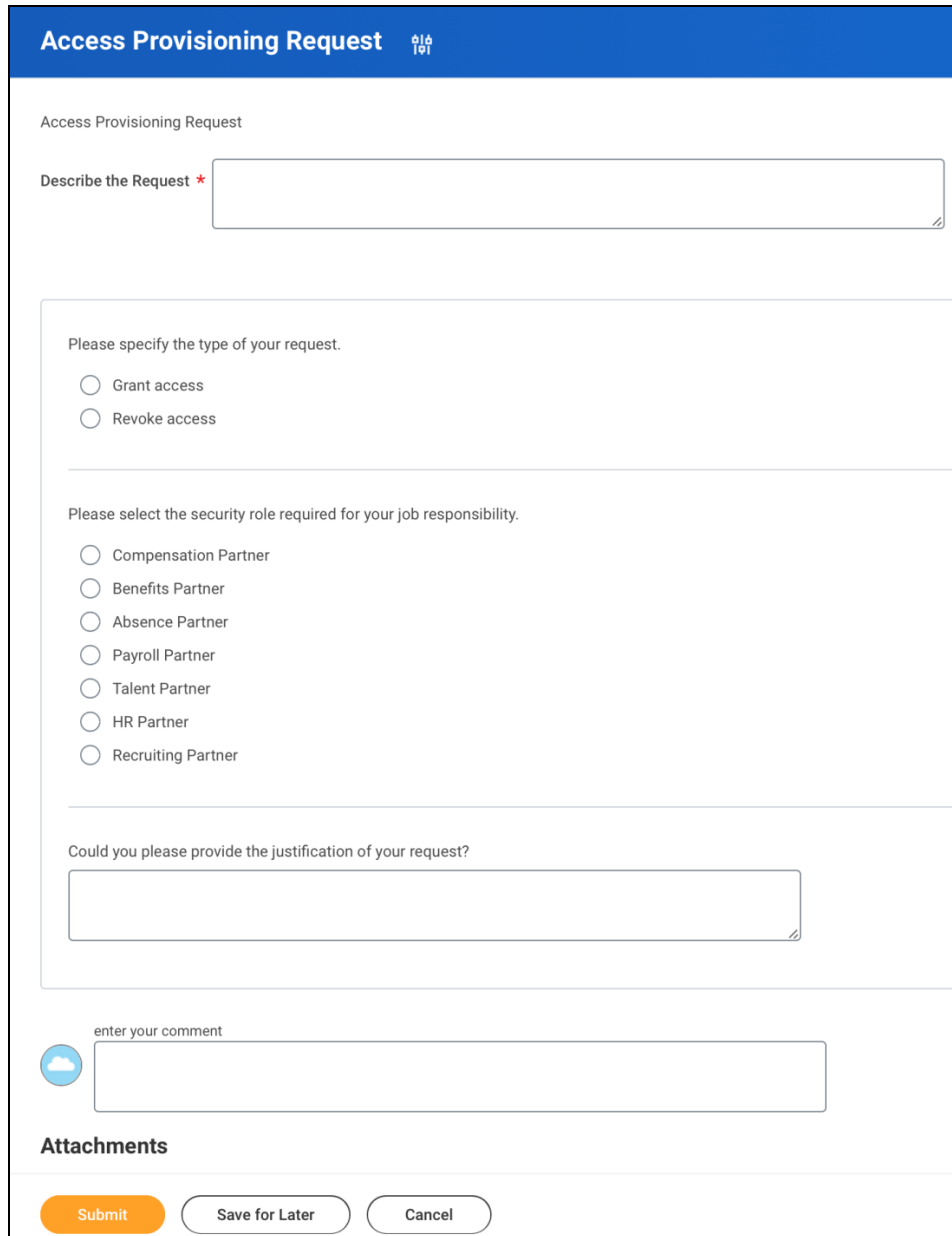



Fig 2: Questionnaire Details page where type and allowed business process can be specified



**Access Provisioning Request** 

Access Provisioning Request

Describe the Request \*

Please specify the type of your request.

Grant access  
 Revoke access

Please select the security role required for your job responsibility.

Compensation Partner  
 Benefits Partner  
 Absence Partner  
 Payroll Partner  
 Talent Partner  
 HR Partner  
 Recruiting Partner

Could you please provide the justification of your request?

enter your comment

**Attachments**

Fig 3: Questionnaire sent to the requestor when Request is initiated in Workday

Workday enables the linkage of questionnaires to the Request Business Process via Request Types. The 'Access Provisioning Request' type can be created using the 'Create Request Type' task in Workday, allowing administrators to configure it by linking it to a questionnaire of the same name and selecting security groups authorized to initiate, view, and correct request resolutions.

Edit Request Type
Access Provisioning Request

**Request Type Name** \*

**Description** \* 

Format B I U A :≡  
 Access Provisioning Request

**Workday Object**

**Questionnaire** × Access Provisioning Request :≡

**Request Description Display** \* × Require :≡

**In Use**

**Inactive**

**Allow Request on Behalf of Person**

**ID Generator**

**Security Configuration**

**Initiate** × Employee As Self :≡

**View All**

× Absence Administrator :≡  
× Benefits Administrator :≡  
× Business Process Administrator :≡  
× Compensation Administrator :≡  
× HR Administrator :≡  

MORE (4)

**Correct** × Business Process Administrator :≡

Fig 4: Request Type configuration with link to Questionnaire and Security Configuration

Workday’s capabilities allow the integration of requests within a business process framework, simplifying the management of requests throughout the organization [7]. The request business process can be defined to govern how users create, approve, and close requests within Workday [7]. Each request type can be managed using rule-based business process definitions, ensuring that when a user initiates an “Access

Provisioning Request” via ‘Create Request,’ it follows the predefined workflow of the corresponding business process.

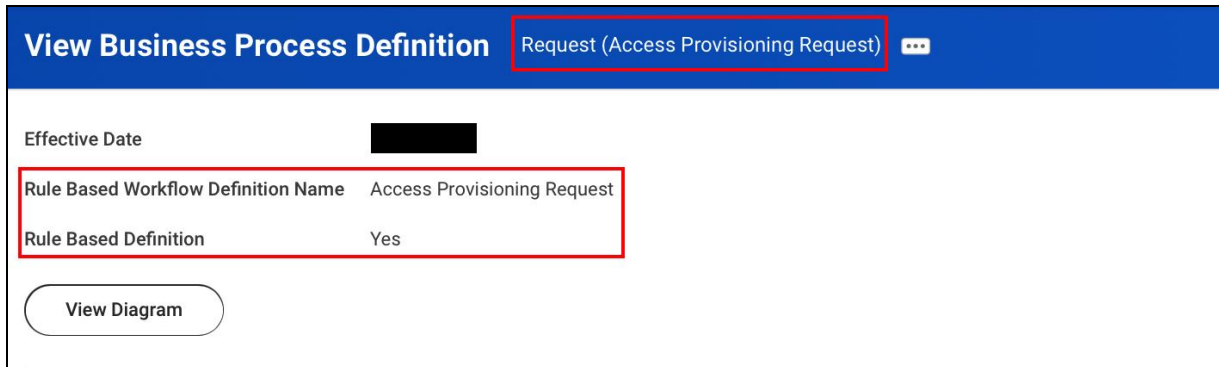


Fig 5: Header section of the Request Business Process definition for Access Provisioning Request

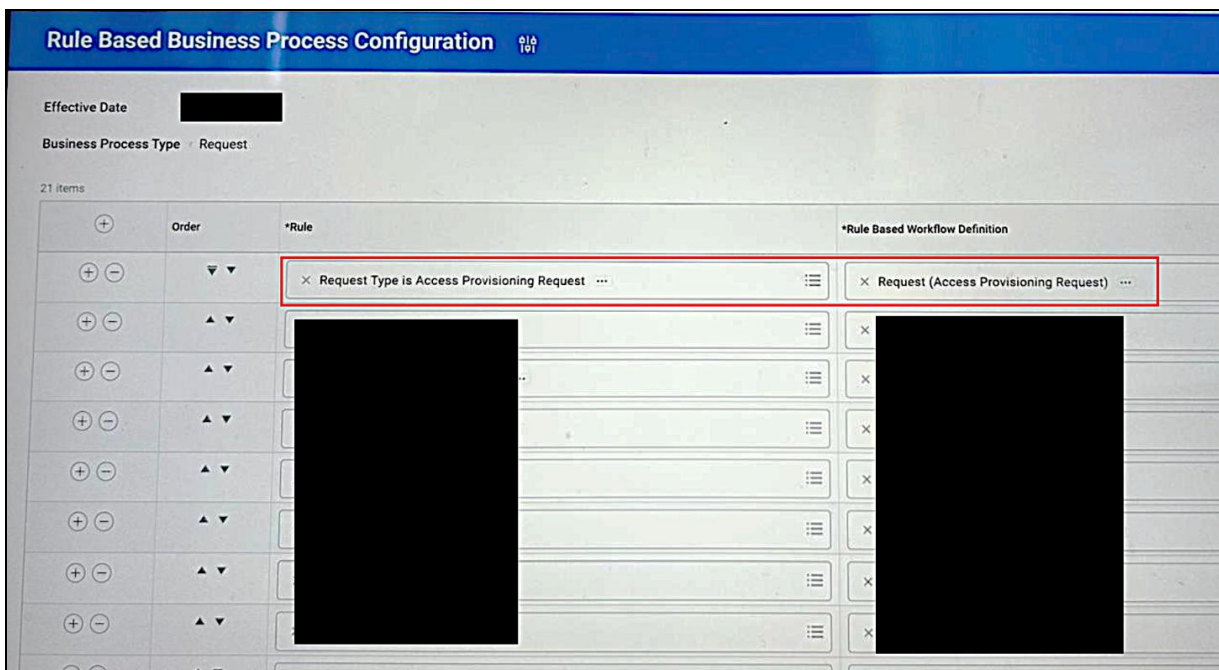


Fig 6: Rule based configuration for Request Business Process

Combining Questionnaires, Request Types, and Request Business Processes establishes a robust framework for managing security access requests and approvals within the Workday HCM system. Employees can submit access requests that adhere to an approval workflow defined within the business process, directing approvals to the appropriate functional owner based on the requested role.

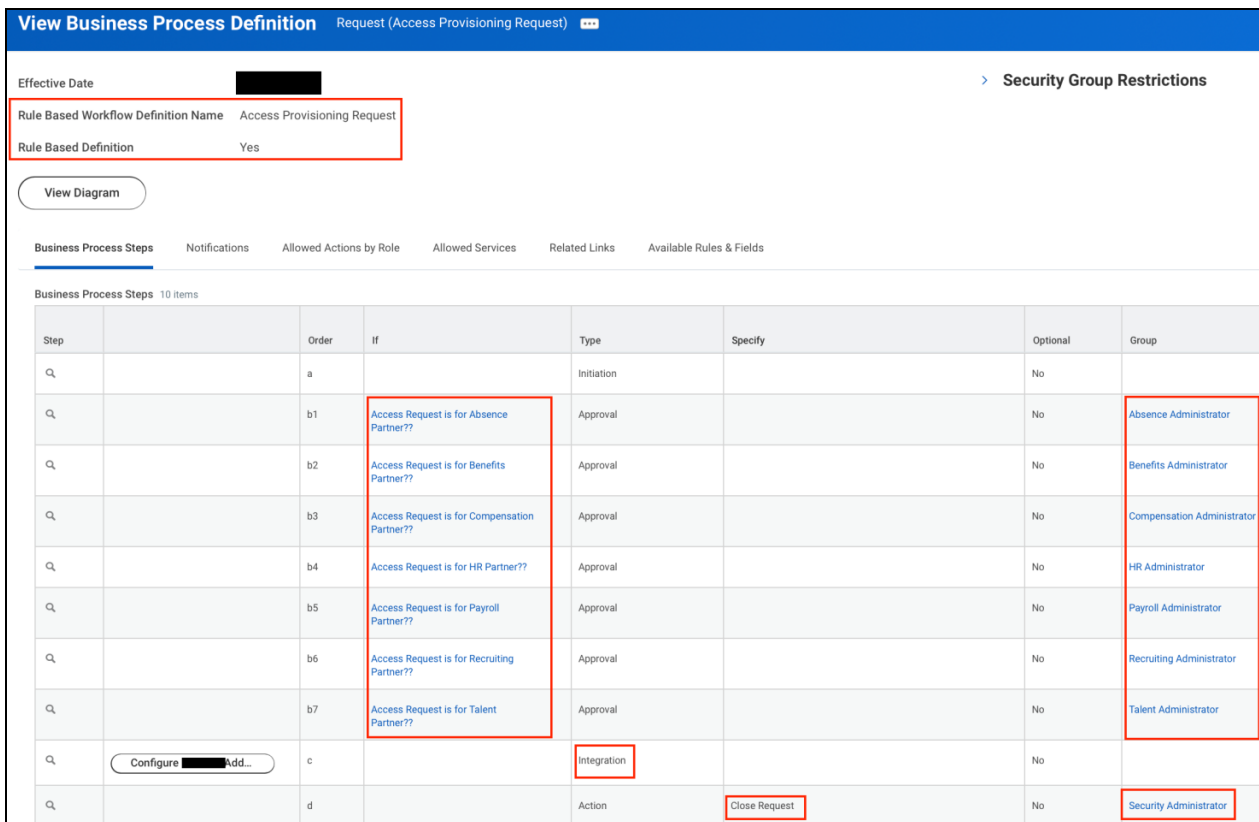
### 3.2 Workday Studio Integration

While establishing an access request and approval framework within Workday HCM is crucial, it is equally important to automate security entitlement provisioning to prevent human errors and data breaches.

Workday Studio allows organizations to develop, manage, and support sophisticated integrations hosted and operated by Workday [5]. These integrations can be automatically triggered as part of a business process [5].

Workday provides an extensive suite of APIs to extract, add, or update data [9]. A custom Workday Studio Integration, leveraging these APIs, can facilitate the automatic granting or revoking of user security based on approved access requests. For instance, the 'Assign Roles' operation of the 'Staffing' web service and the 'Put\_Assign\_User-Based\_Security\_Group' operation of the 'Human Resources' web service can be used to update user security according to approved access requests [9].

The figure below demonstrates the business process definition for the 'Access Provisioning Request' type, incorporating conditional approval steps that direct approvals to the appropriate functional owner based on the requested security role. It also features an integration step that provisions the approved security request using Workday APIs. The final step involves the Security Administrator verifying the security assignment completed by the integration before marking the request as complete.



Step	Order	If	Type	Specify	Optional	Group
Q	a		Initiation		No	
Q	b1	Access Request is for Absence Partner??	Approval		No	Absence Administrator
Q	b2	Access Request is for Benefits Partner??	Approval		No	Benefits Administrator
Q	b3	Access Request is for Compensation Partner??	Approval		No	Compensation Administrator
Q	b4	Access Request is for HR Partner??	Approval		No	HR Administrator
Q	b5	Access Request is for Payroll Partner??	Approval		No	Payroll Administrator
Q	b6	Access Request is for Recruiting Partner??	Approval		No	Recruiting Administrator
Q	b7	Access Request is for Talent Partner??	Approval		No	Talent Administrator
Q	c		Integration		No	
Q	d		Action	Close Request	No	Security Administrator

Fig 7: Complete definition of the Request Business Process: Access Provisioning Request'

### 3.3 Process Flow

The process initiates within the Workday HCM system, where users submit their access requests using the 'Create Request' task. Users must indicate whether the request is to grant or revoke a security role, specify the required security role, and provide justification for the request. Once the request is initiated, it is routed to the relevant functional owner for review and approval based on the requested security role. Upon

approval, a custom integration is launched from the business process to provision the access request within the HCM system. The final step involves the Security Administrator validating that the approved access request aligns with what is granted or revoked in the system before marking the request as complete.

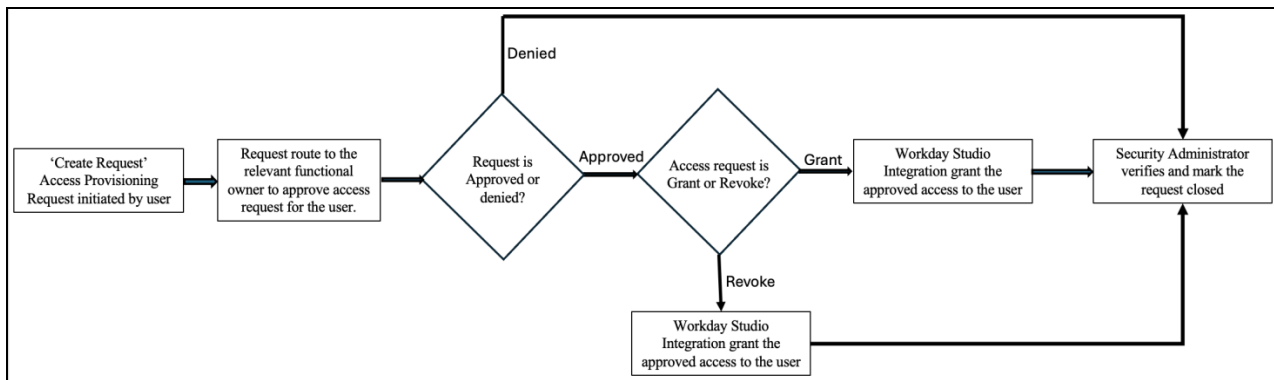


Fig 8: Process flow of access request initiation, approval, and provisioning

#### IV. LIMITATIONS AND FUTURE SCOPE

The proposed custom solution, designed to streamline and automate the processes of requesting and approving user access within the Workday HCM system—an environment that manages sensitive and confidential employee data—exhibits certain critical limitations that merit consideration. The following points delineate the primary constraints of this approach:

- This solution is architected to automate the procedural workflow for security access management within the Workday HCM system, with an ideal scenario where access is granted exclusively via integrated mechanisms following approval from designated authority figures. However, the system's reliance on integration exposes it to potential failure scenarios, wherein manual intervention by security administrators may be required to provision access. The inherent power vested in security administrators to manually override or adjust access levels poses a significant risk, as it introduces the possibility of security access being granted without requisite approvals, thereby compromising the integrity of the approval process.
- Furthermore, while the solution is tailored to the specific task of managing the assignment and revocation of security roles within the Workday HCM framework, it lacks an embedded audit or verification mechanism to ensure that the underlying security infrastructure remains unaltered without explicit, approved requests from relevant functional owners. For example, if the security permissions associated with a compensation partner are inadvertently or deliberately elevated, this could result in unauthorized expansion of access rights across existing user profiles without any formal notification to the functional owner overseeing the compensation domain.

These identified limitations underscore the need for future research and enhancement of the system. A pivotal area for future development would involve the creation of additional custom integration processes designed to mitigate the risks and shortcomings highlighted above. Specifically, the implementation of a sophisticated notification and alert system is recommended. This system would automatically disseminate alerts to IT leads, managerial personnel, and functional owners whenever there are any alterations in user



security access—whether access is granted or revoked—without an officially sanctioned request, thereby ensuring that any manual interventions by security administrators are subject to scrutiny. Additionally, it is imperative to generate real-time alerts for these stakeholders whenever there is a modification in the security access configuration of any role, thereby empowering the relevant groups to conduct immediate validations of any security elevation or demotion actions, ensuring the preservation of the system's integrity and compliance with organizational security protocols.

## **V. IMPACT**

The implementation of a custom integrated and automated solution for security role requests, approvals, and provisioning within the HCM system significantly enhances data access control and policy enforcement within an organization. Traditionally, security access requests are initiated, managed, and approved outside the HCM system, providing minimal visibility for the HR team. Moreover, the manual provisioning of these requests by security administrators can result in unauthorized access or excessive access due to human error.

The custom solution, designed and developed using the tools and features of the cloud-based Workday HCM system, leverages the inherent security mechanisms of the system, making it more robust. The components of this solution, including Questionnaires, Request Types, and Approvers within the 'Access Provisioning Process' business process, are controlled through Workday's security groups. For instance, compensation-related access requests are directed to the 'Compensation Administrator' defined within the Workday system, thereby eliminating the risk of errors associated with email-tracked access requests. Additionally, request types can be restricted to specific groups within the organization, ensuring that unnecessary access requests are not submitted. For example, facilities personnel can be restricted from accessing PII data in the HCM system by limiting their ability to use the access request forms.

A notable advantage of this solution is the facilitation of easy reporting and auditing of access requests, approvals, and provisioning. Custom reports can be generated using standard Data Sources in Workday, such as 'All Requests,' 'Business Process Transaction,' and 'All Transaction Log Entries.' These reports enhance HR team visibility over security assignments within the HCM system, ensuring that no employee has access to sensitive data without the requisite approvals. This heightened control and oversight further ensure compliance and security within the organization.

## **VI. CONCLUSION**

### ***Enhanced Security and Compliance:***

- The integration of an automated solution for security role requests, approvals, and provisioning within the Workday HCM system significantly strengthens data access control.
- Traditional methods of handling access requests outside the HCM system pose risks, including unauthorized access and human error.

### ***Robust Framework:***

- Utilizing Workday's tools such as Questionnaires, Request Types, and Rule-based Business Process Workflows creates a secure and efficient process for managing access requests.

- The custom solution leverages Workday's inherent security mechanisms, making the process more reliable and error-free.

***Automation and Reduced Human Error:***

- Workday's extensive APIs and Studio Integration automate the provisioning of security roles, reducing the likelihood of manual errors.
- Automated processes ensure that security roles are granted or revoked accurately, adhering to organizational policies.

***Improved Visibility and Control:***

- The solution provides comprehensive visibility and control for HR teams, allowing them to track, report, and audit security modifications effectively.
- Custom reports generated using Workday's standard Data Sources enhance transparency and accountability.

***Facilitates Reporting and Auditing:***

- Detailed reports and audit trails within the HCM system facilitate easier monitoring and reconciliation of security assignments.
- This capability ensures that no employee has access to sensitive data without the requisite approvals.

***Operational Efficiency and Regulatory Compliance:***

- The integrated system supports overall operational efficiency by streamlining the access request process within the HCM system.
- Ensures compliance with organizational policies and privacy regulations, protecting sensitive employee data.

By adopting this advanced, integrated system for managing sensitive information, organizations can better protect their workforce's personal data, uphold data integrity, and maintain a robust security framework.

**REFERENCE**

1. Hrlineup, "HRIS Security and Privacy Tips | HR LineUp," HR Lineup, Sep. 08, 2022. <https://www.hrlineup.com/hris-security-privacy-tips/>
2. R. Sander and R. Sander, "Top 5 Best Practices for HR Data Security to follow in 2021," Careers in Government, Oct. 07, 2021. <https://www.careersingovernment.com/tools/gov-talk/about-gov/education/top-5-best-practices-for-hr-data-security-to-follow-in-2021/>
3. J. Sands, "Keep your data secure throughout HRIS implementation," Apr. 13, 2020. <https://www.linkedin.com/pulse/keep-your-data-secure-throughout-hris-implementation-jeffrey-sands/>
4. K. Beaver, "How HR can protect employees' personal information," HR Software, Jun. 24, 2022. <https://www.techtarget.com/searchhrsoftware/tip/How-HR-can-protect-employees-personal->

information#:~:text=Keep%20an%20access%20record,security%20policies%20and%20compliance%20requirements

5. "Concept: Workday Studio", Jun. 17, 2022. <https://doc.workday.com/admin-guide/en-us/workday-studio/studio-fundamentals/ebp1499866049976.html?toc=1.2>
6. J. R, "Top 5 risks when using an email approval process.," Blue Relay, Jul. 04, 2022.<https://www.bluerelay.com/blog/top-risks-when-using-email-for-review-and-approval/>
7. "Setup Considerations: Requests", Jun. 23, 2023. <https://doc.workday.com/admin-guide/en-us/manage-workday/business-processes/requests/fts1549412260404.html?toc=6.7.0>
8. "Steps: Create and Manage Questionnaires", Jun. 23, 2023. <https://doc.workday.com/admin-guide/en-us/manage-workday/business-processes/questionnaires/zhw1611017479991.html?toc=6.6.0>
9. "Workday Web Services (WWS) Directory (V40.2).", Jun. 30, 2023.<https://community.workday.com/sites/default/files/file-hosting/productionapi/versions/v40.2/index.html>
10. J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541–562, Jun. 2013, doi: 10.1016/j.jbi.2012.12.003.
11. "Cloud security and privacy," Google Books.<https://books.google.co.in/books?hl=en&lr=&id=BHazelOuDLYC&oi=fnd&pg=PR7&dq=Enhancing+Data+Protection+and+Compliance+in+Human+Capital+Management+Systems+through+Integrated+Access+Request+and+Approval+Workflows&ots=FC18G4jVJd&sig=N2pS3bTUqJKD5Fcmf6o11qde1UY#v=onepage&q&f=false>
12. Workflow Management Systems: Formal Foundation, Conceptual Design, Implementation Aspects. 1999. [Online]. Available: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4a95012f94f98c1e1071c01fe850fec3ee57813b>
13. "Your Organization's Role in Data Privacy and Security – By Department," AccessCorp, Mar. 27, 2022. <https://www.accesscorp.com/blog/your-organizations-role-in-data-privacy-by-department/>
14. "Risk Management Magazine - Data protection for the HR department," Magazine, Nov. 02, 2015. <https://www.rmmagazine.com/articles/article/2015/11/02/-Data-Protection-for-the-HR-Department>