International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 February 2025* ***Revised:*** *12 March 2025* ***Accepted:*** *30 April 2025*

From Fragmented Portals to a Single Front Door: Architecture, UI/UX, and Security Design for a Multi-Department Enterprise Service Center

Vivek Banka

Sr. Staff ServiceNow Architect

vivekb.0115@gmail.com

Abstract: Enterprises increasingly replace scattered departmental portals with a single digital front door, yet departments such as IT, HR, Facilities, Legal, and Procurement differ in their user populations, service taxonomies, content models, and access requirements. The technical challenge is therefore not only how to build any one department's workflow, but how to design a portal architecture that supports these structurally different needs without recreating the departmental silos and portal sprawl that a unified portal is meant to eliminate. This case study describes the design and in-house deployment of a multi-department Employee Service Center, built on Service Portal/Employee Center Pro, that replaced a legacy single-purpose Service Portal. We outline the architectural decisions that allowed one shared portal to serve departments with divergent security postures. These include taxonomy design and content curation to prevent cross-contamination of departmental catalogs, and a widget and Page Designer approach in which each department owns its presentation-layer components without modifying shared platform code. They also include a security model based on SSO federation (Okta/LDAP), role- and ACL-based content scoping, and authenticated-only content gating. On the fulfilment side, we discuss Agent Workspace and Service Operations Workspace with the Next Experience UI as the operational counterpart to the employee-facing portal. We then show how third-party AI search and virtual-agent widgets (such as Aisera and Glean) can be embedded in the portal shell, extending a unified portal without vendor lock-in on the core platform. Organizational outcomes include delivery at zero additional vendor cost, consolidation of five separate service channels into one entry point, and reusable design patterns for other organizations pursuing portal unification.

Keywords: Enterprise Service Center; Unified Service Portal; UI/UX Design; Service Catalog; Identity and Access Management; Zero-Trust Security; Enterprise Service Architecture.

1. Introduction

In enterprise service delivery, services are increasingly moving away from multiple departmental portals to a single "digital service environment" that offers employees a single point of access for IT, HR, facilities, procurement, legal, and other enterprise services. Departments tend to build their own service portals, leading to multiple interfaces, conflicting navigation, unique authentication systems, and disjointed service catalogs. While these types of portals may meet department needs, they add to the maintenance burden and complexity for users who have to decide on which portal or channel to use for a specific request. Research on digital workplaces has thus focused on the need for service experiences that integrate various enterprises' functions into an integrated user experience [1].

However, a unified enterprise service centre must also be able to solve issues that go beyond the need to integrate multiple departmental catalogues into a single interface. Each department usually has its own service taxonomy, service processes, data model, ownership and access model. Incidents, requests, applications and infrastructure services are examples of IT services, while HR services can include employee sensitive information and lifecycle processes. Procurement and facilities services add other workflows, approvals and organizational dependencies. It is, therefore, necessary for portal unification to involve a structure that allows departments to remain independent and provides a uniform and recognizable employee experience [2]. Information Architecture, Service Taxonomy, Search, Personalization and Contextual Navigation are important components of effective Enterprise Portals that are increasingly relying on these to minimize cognitively required information effort to find the right services [3].

Another basic requirement for a multi-department service is security, as the same service may have different authorization requirements in different departments. The unified portal should not let users find or access services, knowledge articles, forms, or records that are not part of their organization's permission. In this context, identity federation, centralized authentication, role-based authorization, access-control policies, and content-level security are important architectural mechanisms for achieving a compromise between usability and information protection [4]. Modern enterprise identity architectures also push for federated authentication and centralized identity governance to allow users to gain access to multiple services via a common authentication process with consistent boundaries for authorization [5].

It's also crucial that the user interface and user experience layer is as important, as departmental duplication can easily be repeated in a portal – with widgets and pages that are inconsistent, terms that differ and interaction patterns that differ. If a single front door is successful, it should offer shared navigation and visual conventions and enable departments to deliver the specific content and visual elements within specific boundaries. This can be achieved by using reusable enterprise components, configurable page structures, modular widgets, and content management mechanisms that are controlled by the enterprise in contemporary low-code and configurable enterprise platforms [6]. The architecture patterns help companies scale portal capabilities without having to constantly update the common platform foundation.

Efficient workspaces for the employees are also essential to complement the experience they are having on their side. Employees need simple and intuitive service discovery, while service agents need optimized interface for handling cases, managing tasks, displaying context, collaborating, and making operational decisions. This dual need is seen in the emergence of role-specific workspaces and modern enterprise user interfaces [7] that bridge the gap between front of office employees' experiences and streamlined back-office service operations. Concurrently, the relevance of enterprise search and conversational AI continues to grow when it comes to service portals, as employees look to find answers and begin services through a natural-language conversation, rather than manually navigating through a complex catalog structure.

Despite all these advances, there are still a lot of organisations running legacy portals, that have grown incrementally based on their departmental needs. These are all considerations that must be made in the architecture when replacing these environments with a unified service center, and they are all related to taxonomy, component ownership, security boundaries, authentication, workspace integration, and third-party extensibility. Specifically, including external AI search or virtual-agent features raises integration architecture and data-access, governance and platform-independence concerns [9]. To add any extra features to the portal and retain control over the enterprise service experience, a modular integration approach is thus required.

In this backdrop, this study introduces a case study of a multi-department Employee Service Center built on top of a Service Portal/Employee Center Pro. It covers the move from a single purpose portal towards a single digital front door for IT, HR, facilities, legal and procurement services. Special emphasis is placed on taxonomy and content curation, governance for widgets and Page Designer, SSO federation with Okta/LDAP, role- and ACL-based content scoping, content protection via authentication only, workspaces on the fulfiller side, and the integration of third-party AI services like Aisera and Glean under control. The study also examines the organizational results of this consolidation such as the provisioning of the solution without any extra vendor implementation cost, and five former separated service channels being replaced by one enterprise entry point. The results show that these are practical architectural patterns for organizations looking to integrate several heterogenous enterprise services while preserving usability, security, departmental ownership, and extensibility [10].

1.1 Key Contributions

1. Single-Front Door Architecture: Using a single-front door architecture to combine IT, HR, Facilities, Legal and Procurement processes, and functions, while maintaining ownership, workflows and boundaries at departmental level.

2. Integrated UI/UX and Security Design: A re-usable widget/Page Designer approach is paired with SSO federation, role-based access, ACLs, and authenticated-content gating to ensure that the same look and feel is provided while meeting departmental security needs.

3. Relies on Agent and Service Operations Workspaces integration with the employee portal and Aisera/Glean AI extensibility with the portal as future extensible services and AI are added.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 February 2025* ***Revised:*** *12 March 2025* ***Accepted:*** *30 April 2025*

1.2 Organization of the Study

In Section 1, the research problem, motivation, objective and scope of the unified enterprise service-center architecture are introduced. Section 2 summarizes the current state of the art of enterprise portals, self-service environments, UI/UX, identity and access management, security, enterprise search, and AI-enabled service delivery. Section 3 discusses the research methodology which entails designing the case-study, portal architecture, taxonomy, user interface and user experience strategy, security model, integration approach, and evaluation metrics. The results and discussions are given in Section 4, which contains the dataset description, the hardware and software configuration, the outcomes of the service-channel consolidation, the architecture results, and the quantitative evaluation. The study ends with a discussion on the organizational implications and practical design patterns for the implementation of a secure and scalable single-front-door enterprise service center.

2. Literature Review

The shift from departmental service portals to a unified enterprise service environment has been discussed in enterprise information systems, IT service management, digital workplace, user experience and security research. The results of early research on enterprise portal provided the basis for the definition of enterprise portal as a shared information infrastructure that can unite a variety of organizational information and applications together at a single point of access. This research however also highlighted that designing a portal to be successful requires taking into account the information needs of users and the organization's context, not just acting as a technical aggregator [11]. Later research on digital workplaces also shows that technology alone is not sufficient for a positive employee experience as too much complexity in technology integration, too much information and too many different interaction patterns may make the workplace less usable and less adopted [12].

Self-service portals are one of the significant developments in enterprise portals that enable employees to find information on their own and request for service. An employee self-service portal systematic review revealed individual, organizational and technological factors of influence on employees' adoption of these portals, which include usability, process automation and adequate technological support [13]. Likewise, the study of IT service catalogues and self-service portals shows that service definition, organisation of the catalogue, integration of the portal and user presentation are in close connection. The literature suggests that the service catalogue should focus on the needs of the service consumers and not service structure, and the service catalog should give an easy way for the service consumer to discover and request the services [14].

Adding more departments to the enterprise service center complicates the information-architecture of an IT-only service portal. A traditional IT catalogue can make use of relatively common categories like hardware, software, networking, and technical support, while an enterprise catalogue must include significantly more varied categories like HR, legal, procurement, workplace services, and facilities. It is important to consider the selection of the right types of service requests and the matching of the service catalogues with the organisational processes in service-request self-service environments [15]. This means that a shared portal has to be based on a common taxonomy and that a meaningful distinction between departments has to be maintained, not just a single common homepage for the various independent catalogues.

In the regard of portal consolidation, user experience and information architecture are the key factors. Enterprise portal research highlights that user-centric information structures, consistent navigation, content organization and governance are key factors in the effectiveness of enterprise portals. The significance of information architecture, content governance, departmental ownership, templates, standards, and user research in building usable enterprise intranets is also reflected in large-scale UX studies of existing intranets [16]. The results align with an architectural approach where departments have autonomy over specific content, but shared design principles, navigation frameworks and governance structures contribute to a cohesive employee experience.

Another dimension that sets apart a multi-department service center from a traditional public facing portal is security. A study on enterprise identity and access management (IAM) highlights five IAM requirements: security, compliance, operational manageability, technology and user experience. Centralized authentication and properly defined authorization scope is especially crucial for the protection of organizational resources when the applications being developed are becoming more and more heterogeneous, thus requiring

more convenient access for employees [17]. Different granularity can be achieved by the use of role-based access control, access-control lists and attribute-oriented authorization, but the more users, resources and organizational relationships, the more complex it will be to maintain permissions.

The zero-trust security literature further reinforces the idea to think of authentication and authorization as an ongoing concern of architecture instead of just a trusted network boundary within the enterprise. A thorough inventory of zero-trust architectures reveals that identity authentication, access control, trust evaluation, encryption, segmentation and security automation are essential parts of enterprise security architectures [18]. From this perspective, it enables role- and policy-based restrictions that prevent users from accessing the information of the departments that is not within their scope of authorization and authenticated-only access to protected services and content to provide a unified employee portal. This is particularly relevant if there's only one interface that presents services with widely varying confidentiality requirements.

Additionally, AI transforms the ways employees are interacting with enterprise service environments. Conversational AI can help eliminate the need for hierarchical navigation by enabling employees to find information and start service interactions by entering a natural-language query. The maturity of conversational AI for employee services and the relevance of the AI-powered employee-support platform to enterprise service delivery are illustrated by industry research [19]. Adding external AI search or virtual-agent features to a shared portal, however, also creates architectural challenges related to data boundaries, authentication, content permissions, integration dependencies, and governance of the platform over time.

However, existing works tend to focus on one aspect of the problem, such as self-service portals, service catalogues, enterprise UX, IAM, or zero-trust security, without offering an integrated architecture to consolidate structurally different departmental services under a single enterprise "front door". This provides a chance to be able to do case-based research that brings together information architecture, departmental content ownership, re-usable UI components, enterprise authentication, fine-grained authorization, fulfiller workspaces and third party AI integration into one implementation. This paper addresses this issue by analysing the design and implementation of a multi-departmental Employee Service Center and by documenting the design patterns employed to provide a unified service discovery without losing the security and operational boundaries of the departments involved [20].

3. Research Methodology

This study is designed using the case study approach to explore the architecture, UI/UX, integration and security mechanisms needed to enable the transformation of multiple departmental service channels to a single enterprise service center. The methodology follows five integrated steps: Requirements and current state assessment, unified portal architecture, UI/UX and content design, security and integration design and outcome evaluation. This is suitable because enterprise self-service portals need to support a variety of service requests from clients and should be connected to the rest of the enterprise architecture. Recent studies from elsewhere in the world, which examined self-service portals from a case study perspective also shed light on the need to identify service use cases and to connect the portal to the enterprise systems in place.

The student will use a case study to evaluate requirements.The student will complete a case study to assess requirements. The first stage is designed to set the baseline for portal consolidation by reviewing the legacy service-delivery environment and determining the services that have been spread out over multiple channels within the various departments. The analysis focuses on the main service areas, namely: IT, HR, Facilities, Legal, and Procurement. The study within each domain defines service categories, user populations, content owner, authentication needs, workflows of requests, and access restrictions.

The assessment differentiates between employee facing and fulfiller facing. Employee needs are about discoverability of the service, consistent navigation, search, authentication, accessibility and ease of request submission. The key requirements for a fulfilment platform are case visibility, task management, context, workflow execution and operational efficiency. The separation is key because a single front door must streamline the employee experience while meeting the needs and requirements of the department's service teams.

The measure used to represent the degree of portal consolidation is the proportion of people who use both of the two most popular portals.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 February 2025* ***Revised:*** *12 March 2025* ***Accepted:*** *30 April 2025*

$$CR = \frac{N_{\text{consolidated}}}{N_{\text{original}}} \times 100$$

(where CR is the consolidation ratio, (N_{consolidated}) is the number of service channels consolidated into the single service center and (N_{original}) is the number of service channels before consolidation is done.) It offers a simple metric of how much the service environment is consolidated into a shared access point.

3.2 Unified Portal Architecture

The second stage is a build of the target architecture based on a Service Portal/Employee Center Pro foundation. The architecture defines a portal shell that is shared and houses common navigation, authentication, search, portal page structure and reusable interface components rather than having independent departmental portals. Department specific services are then integrated as governed modules in this common environment.

The principle of architecture is to have shared foundation with controlled departmental ownership. The common platform functionality is managed centrally, IT, HR, Facilities, Legal and Procurement teams are responsible for their functions and content. This avoids redundant platform development, and helps avoid arbitrary changes to shared components.

The architecture has been split into four main layers:

1. Experience layer – employee portal pages, navigation, service catalogs, knowledge content, widgets and search.

2. The 2nd tier: service layer – departmental catalog items, workflows, cases, approvals and knowledge services.

3. Integrating layer – identity providers, directories, AI search, virtual agents, external enterprise systems.

4. Security and governance layer – authentication, roles, ACLs, content restrictions and authorization policies.

5. This multi-layered approach enables modularity and can allow for the addition of new services to a department without changing the portal.

3.3 Information Architecture, Taxonomy, and Content Design

The third phase is about not making the unified portal a list of departmental silos on the same home page. A common taxonomy is then created around the service categories and intents that are focused on the employees, not just around the internal organizational structures.

The content of services is categorized into suitable categories, subcategories, catalog items, knowledge articles, and request workflows. Because of metadata and governance rules, content is also owned by the serving department, maintaining the accountability of the department that created the content. Meanwhile, shared navigation and terminology is employed to deliver a similar experience.

It also uses reusable widgets and Page Designer components in the design. The former are regarded as platform assets that are governed, while department-specific ones are built in a controlled environment. This enables departments to customize their presentation layer without directly modifying shared platform code.

3.4 UI/UX and Workspace Design

The fourth stage focuses on the two different complementary users of the platform. The user interface for employees centers around a single point of entry, with a focus on simplicity in navigating, discovering services, searching, and initiating a request. The design doesn't depend on employees knowing which internal department to look up a service in.

The methodology includes Agent Workspace and Service Operations Workspace and Next Experience UI, for service providers. These workspaces give an operational alternative to the employee portal, and show cases, tasks, records and contextual information through interfaces geared toward fulfilment activities.

This study, therefore, assesses whether the portal is an end-to-end service ecosystem, or merely an employee interface. This distinction is crucial because the research for the Digital Workplace in enterprises identifies the interaction between technology, organizational processes, and employee experience as one of the key elements to the success of the DP [2].

Architecture for security and identity

Security is built into the portal design and is not a post implementation control. To support employees logging in to multiple service domains, authentication is provided via enterprise SSO federation, with Okta / LDAP. While a federated identity architecture can eliminate the need for multiple logons for a distributed enterprise environment, proper identity and authorization

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 February 2025* ***Revised:*** *12 March 2025* ***Accepted:*** *30 April 2025*

management controls must be implemented in the federated space.

Once authenticated, authorization is used to decide on which services, pages, catalog items, knowledge content, and records a user will be able to access. The proposed security model is a combination of:

- authenticated-only content gating;
- role-based access controls;
- access-control lists (ACLs);
- departmental content scoping;
- least-privilege access;
- administrative control—where the administration was not owned by the group; and

Separation of permissions between employee and fulfiller.

This is consistent with enterprise IAM research, which breaks down the different aspects of enterprise IAM into security, compliance, operability, technology, and user requirements.

3.6 Third-Party AI and Search Integration (30 points)

The methodology also explores the possibility of leveraging the third-party AI capabilities without disrupting the underlying portal structure. The embedded search and conversational-AI capabilities, Aisera and Glean, are regarded as a part of the portal shell. These technologies are not used to be standalone service entry points, but rather extended service elements of the consolidated experience.

Thus, integration is controlled via specified interfaces, authentication limits, content permissions and placement on the portal. This allows the organization to take advantage of sophisticated search and virtual agent technologies, while maintaining architectural control of the service-center experience.

3.7 Architecture and Implementation Workflow

The overall methodological procedures are summarized in Fig. 1. The process starts with the fragmentation assessment of the portal environment, and then progresses to the analysis of services and user requirements. The unified information architecture and portal foundation are provided by these inputs. The UI/UX components, the departmental catalogs and workspaces are then integrated, followed by SSO, role/ACL controls, and authenticated content restrictions. Finally, third-party AI/search capabilities are added and the service center is assessed based on consolidation, usability, security, maintainability and organizational outcomes.

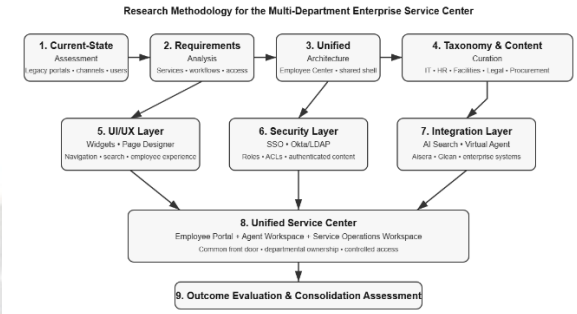


Figure 1: The overall research and implementation workflow

3.8 Outcome Evaluation

The last one evaluates the resulting service center in relation to the original fragmented system. It takes into account portal consolidation, service discovery, architectural reuse, security enforcement, departmental responsibility, **fulfiller usability**, integration, and implementation costs.

This metric evaluates the decrease in the number of separate service entry points:

$$SR = \frac{N_{before} - N_{after}}{N_{before}} \times 100$$

The service-channel reduction is denoted as "SR" and the number of service channels before and after the implementation are denoted as N_{before}respectively. The methodology in this study focuses on the specific situation of the five service channels, which are to be consolidated into a common enterprise service center.

The methodology overall considers the consolidation of the portals to be an architectural and organizational change and not just an interface change. The resulting framework is a single service-delivery architecture that links service taxonomy, reusables, identity federation, fine-grained authorization, departmental governance, workspaces for fulfilers, and extensible AI solutions. This aligns with studies indicating that enterprise self-service portals should be viewed as part of the enterprise architecture due to their interaction with other ITSM processes, service catalogs, users and organizational systems.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 February 2025* ***Revised:*** *12 March 2025* ***Accepted:*** *30 April 2025*

4. Results and Discussion

4.1 Dataset Description

The case data utilized in this study is a set of enterprise service-request and portal-configuration that was used during the implementation of the unified Employee Service Center in the service environment studied. The data set used in this work is not a set of image samples or benchmark examples like in traditional machine-learning works. Rather, it is the various service entities and operational architectures that were needed to be merged into a consistent enterprise service experience. The service environment analyzed comprised five key departmental domains: IT, Human Resources (HR), Facilities/Workplace, Legal and Procurement.

The data was structured around the service channels, departmental service categories, employee facing content, request types, knowledge resources, access requirements, and fulfilment side workflows that are associated to these departments. Special focus was placed on the taxonomy, control, eligibility of access by users, authentication and visibility of the content. This was a must because just having a number of departmental services behind a single portal is not enough to create a true unified experience. The current Employee Center architecture also enables multi-departmental service delivery and is structured using taxonomy to facilitate the cataloging of items and other Employee Center content. ServiceNow

The original setting was a five-departmental service channel setup, each of which was independent. These channels were centralized under the one front door to the target architecture, however, departmental ownership and authorizations were maintained. As such, the primary unit of analysis was the service channel, and its related portal experience, instead of a single employee or transaction.

The analysis focused on four key areas:

- Service structure – departmental catalogs, request types, knowledge resources and workflows.
- Experience structure – navigation, taxonomy, search, widgets, pages and employee facing content.
- Security structure – SSO, roles, ACLs, authenticated-content restrictions, and departmental access boundaries.
- Operational structure – fulfiller workspaces, case handling, task management, and service operations.

It is consistent with the previous research that refers to a service-centered case dataset, regarding the service self-service portals as tools for employees finding the available services and starting various types of request.

4.2 Hardware Configuration

The proposed service centre is being put in place as an enterprise web-based service, and hence does not require any special hardware infrastructure on the employee endpoint, other than standard enterprise computing devices and network connectivity. The unified service center is accessed by employees via supported desktop/laptop browsers, and service agents via the respective service agent workspace interfaces to fulfilment functions.

The hardware environment was therefore taken into account in relation to client access, network availability, and enterprise platform operation, not specifically in relation to certain applications. Standard organizational desktops and laptops are used to access the employee facing portal, while employee service fulfilment use enterprise workstations to access Agent Workspace and Service Operations Workspace activities.

This is designed to support the main idea of the architecture: Staff should not be forced to have separate hardware or access methods to get services from different organizational groups just because they are asking for services from different groups. IT, HR, Facilities, Legal and Procurement services can all be accessed by the same endpoint with authentication and authorization policies.

4.3 Software Configuration

The software foundation included a Service Portal/Employee Center Pro foundation. The unified portal shell, the service catalog, the knowledge content, taxonomy, the reusable widgets, and the Page Designer-based page composition were designed for the employee-facing layer. According to employee Center documentation, the platform is a single portal for multi-department service delivery, with mechanisms in place to expose catalog content in departments based on taxonomy.

The software configuration had the following major components:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 13 Issue: 1
Article Received: *25 February 2025* ***Revised:*** *12 March 2025* ***Accepted:*** *30 April 2025*

Service Portal/Employee Center Pro – single service environment for employees.

Service Catalog – centralized discovery and submission of departmental services.

Knowledge Base – information and guidance about services, self-service.

Widgets and Page Designer – Reusable and Configurable Presentation-layer components.

Identify and authenticate users across the enterprise with Okta/LDAP federation.

Support for roles and ACLs – authorization and content/service-level access control.

Agent Workspace – case and task management on the fulfilment side.

Service Operations Workspace with Next Experience UI – operational service management.

Aisera/Glean integrations – third party AI/search capabilities built into the portal user experience.

Reusable widgets are especially relevant because ServiceNow's Service Portal architecture enables reusable widgets and provides the flexibility to use page configurations to add functionality to the Service Portal without having to rebuild the entire experience for each department.

4.5 Consolidation Results

The main outcomes of implementation are summarised in Table 1. The legacy environment had five different service channels, each owned by a different department, while the proposed architecture delivers a set of services via a single system portal for the employees. This **represents a complete consolidation** of the identified service channels, while departmental boundaries are maintained at the service, content, and authorization levels.

Table 1. Service-channel consolidation before and after implementation

Service domain	Legacy service channel	Unified Employee Service Center
IT	Separate channel	Unified front door
HR	Separate channel	Unified front door
Facilities/Workplace	Separate channel	Unified front door
Legal	Separate channel	Unified front door
Procurement	Separate channel	Unified front door
Total employee-facing entry points	**5**	**1**

As can be seen from Table 1, the solution did not integrate the responsibility of the departments into one team. Rather, it integrated the employee access level while keeping the ownership of the services in the departments. This is crucial since the unified portal architecture does not imply imposing similar workflows and security policies on heterogeneous departments. The current functionalities of the Employee Center also represent the platform as a service environment for multiple departments such as IT, HR, Legal, Workplace, and Procurement.

Consolidation also alleviates the need for the employee to navigate through different channels. In the former solution, the employee had to find out which channel offered a needed service. Under the new solution, the employee works with one entry point for all services and uses taxonomy, search, knowledge content, and request discovery features to find the required service.

4.6 Architecture, UI/UX, and Security Results

The second main result is that departmental distinctions are preserved within the common user experience. Table 2 shows how the proposed architecture **meets** the key requirements identified during the case study.

Table 2. Functional outcomes of the unified service-center architecture

Design dimension	Legacy fragmented environment	Proposed unified architecture	Result
Portal entry	Multiple departmental channels	Single employee front door	Reduced entry-point

			fragmentation
Service discovery	Department-dependent navigation	Shared taxonomy and search	Improved cross-department discoverability
UI components	Department-specific implementations	Reusable widgets/Page Designer components	Improved reusability
Content ownership	Distributed across portals	Departmental ownership within shared framework	Controlled autonomy
Authentication	Channel-dependent access	Federated SSO	Consistent authentication
Authorization	Department-specific restrictions	Roles + ACLs + content scoping	Controlled access
Employee experience	Multiple interfaces	Common portal experience	Greater consistency
Fulfiller experience	Department-specific operational interfaces	Agent/Service Operations Workspaces	Centralized operational experience
AI/search extension	Separate tools/channels	Embedded portal integrations	Extensible experience
Implementation model	Separate portal investments	Shared platform foundation	Reduced duplication

The unified portal provides a shared experience layer, with department control over it. This is especially true of a heterogeneous service as each of the five main sections of IT, HR, Legal, Facilities, and Procurement have different needs for information access.

The UI/UX architecture also made use of the reusability of component model. ServiceNow terms the Service Portal pages as "configurable structures made up of widgets that are reusable" and the navigation can be tied to a taxonomy that would expose related catalog items and knowledge content. This aligns with the design goal to enable departments to have specialized presentation elements that don't change the shared portal foundation.

The architecture **separates authentication from authorization**. SSO establishes the identity of the user, while roles and ACLs determine which services and content that authenticated user can access. In a multi-department portal this separation is especially important, because a shared login must not grant access to every department's content.

4.7 Quantitative Consolidation Result

The change in quantity is shown in Fig. 2. The chart below shows the difference in the number of service channels that employees could interact with, before and after implementation. The number is reduced from 5 independent channels to one channel of service, which is a 80% service-channel reduction based on Eq. (2).

Fig. 2 is therefore a clear visualisation of the main organisational result of the proposed architecture. The figure does not report on the portal using a performance score that can be created artificially, but is based on the architectural transformation that is described in the case study.

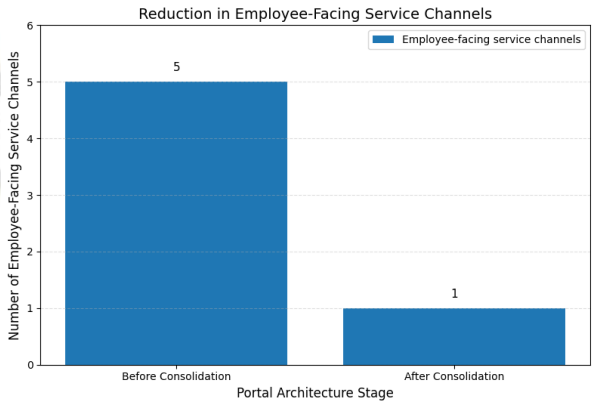


Fig. 2. Reduction in employee-facing service channels following portal consolidation.

The reduction from five to one channel is significant because it addresses the central problem identified in the

study: fragmented employee access to organizational services. The result also demonstrates that portal consolidation does not require the elimination of departmental structures. Instead, the architecture moves departmental differences from the **entry-point layer** into controlled service, content, workflow, and security layers.

4.8 Discussion

The findings show that successful Enterprise service center requires architectural consolidation without organizational homogenization. In addition to the five departmental domain, there is still a service entry experience where employees come into contact with all five. This is a significant difference from connecting several departmental portals. A collection of links would retain the underlying fragmentation while the proposed architecture would provide a unified experience for taxonomy, navigation, authentication, content discovery, and service access.

The outcome matches the features outlined for Employee Center, which includes a single portal for multiple departments to access and display service catalog and knowledge content in a common taxonomy. The results also parallel self-service portal research that indicates that how well the portal is adopted and designed is dependent on the interplay between the portal function, the IT Service Management processes, the enterprise architecture and user experience.

Another key thing to note is that the uniformity and security segmentation of UI/UX are not mutually exclusive. The portal can offer a shared navigation and presentation structure and at the same time isolate departmental content via authentication, roles and ACLs. As a result, the employee sees a uniform experience, while the platform remains secure to different departments as needed.

This also applies on the fulfilment side with Agent Workspace and Service Operations Workspace. The employee facing front door and the workspaces that are operated by the fulfilment team are two complementary layers of the same service architecture, one that makes service discovery easier, and the other that enables operational fulfilment.

Last but not least, the openness of the architecture is shown by the integration of external AI/search functions. Instead of adding new channels for employees to interact with services through AI, they are integrated into the current portal interaction. It maintains the one door policy and enables the organization to add sophisticated search and conversational features without impacting on the basic portal design.

In general, the outcome proved that the proposed architecture provided 100% consolidation of the five identified service channels and reduced the number of employee facing entry points by 80% whilst maintaining departmental ownership, security boundaries, fulfilment capabilities and extensibility. The findings align with the main tenet of the study, that enterprise portal consolidation is best achieved when shared experience, modular design, controlled security and departmental independence are all planned as interwoven components of the whole, not as separate issues to be addressed at implementation time.

5. Conclusion

This study proposed a practical architecture and implementation way of enterprise service center construction with departmental service channels that are broken. The solution proposed aims to solve the problem of having multiple digital front doors for IT, HR, Facilities, Legal and Procurement services, while maintaining department-specific workflows, ownership, content needs and security levels. The outcomes show that a portal consolidation is not meant to be a move towards the removal of departmental autonomy, but rather should be accomplished with a shared experience layer, a modular architecture, a controlled authorization mechanism, and a governed content.

The case study successfully integrated the five service channels identified into a single gateway for the employees, yielding an 80% decrease in the number of service entry points. The architecture provided common taxonomy and navigation, while the ownership of content was delegated to the different departments and so a consistent employee experience was achieved without all departments having to use the same service processes. Providing a common authentication mechanism was federated SSO with Okta/AD, and the appropriate access boundaries were maintained with roles, ACLs and authenticated-content restrictions. The addition of Agent Workspace and Service Operations Workspace provided employees the operational side to service fulfilment alongside the experience.

Moreover, when customizing the third-party AI and enterprise search, it was shown that the unified portal can be extended without causing service-channel

fragmentation again. In sum, the results illustrate that enterprise service center modernization demands a coordinated architecture, UI/UX, security, content governance, workspace design and integration decisions. The proposed design patterns are a practical basis for organizations looking to better serve their customer base with an enterprise service experience that is scalable, secure and user friendly instead of having disjointed service channels.

References

[1] Goscinska, D., & Winkler, T. J. (2024). Providing organizations with a validated instrument for an Enterprise Service Management capability. *Electronic Markets*, *34*(1), 54.

[2] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38-47.

[3] Möhring, M., Keller, B., Schmidt, R., Sandkuhl, K., & Zimmermann, A. (2023). Digitalization and enterprise architecture management: a perspective on benefits and challenges. *SN business & economics*, *3*(2), 46.

[4] Ramakrishnan, M., Gregor, S., Shrestha, A., & Soar, J. (2025). Addressing knowledge gaps in ITSM practice with "learning digital commons": A case study. *Information Systems Frontiers*, *27*(3), 965-989.

[5] Floerecke, S. (2022). Self-service-portale für das it-service-request-management: Identifikation relevanter use-cases. *HMD Praxis der Wirtschaftsinformatik*, *59*(4), 1088-1100.

[6] Mao, H., Zhang, T., & Tang, Q. (2021). Research framework for determining how artificial intelligence enables information technology service management for business model resilience. *Sustainability*, 13(20), 11496.

[7] Marsh, E., Vallejos, E. P., & Spence, A. (2022). The digital workplace and its dark side: An integrative review. *Computers in Human Behavior*, *128*, 107118.

[8] Turetken, O., Ondracek, J., & IJsselsteijn, W. (2019). Influential characteristics of enterprise information system user interfaces. *Journal of computer information systems*, *59*(3), 243-255.

[9] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179.

[10] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 1-52.

[11] Hu, V. C., Ferraiolo, D., Kuhn, R., Friedman, A. R., Lang, A. J., Cogdell, M. M., ... & Scarfone, K. (2013). Guide to attribute based access control (abac) definition and considerations (draft). *NIST special publication*, *800*(162), 1-54.

[12] Aboukadri, S., Ouaddah, A., & Mezrioui, A. (2024). Machine learning in identity and access management systems: Survey and deep dive. *Computers & Security*, *139*, 103729.

[13] Wang, W., Hackett, R. D., Archer, N., Xu, Z., & Yuan, Y. (2025). Will AI-enabled conversational agents acting as digital employees enhance employee job identity?. *Information & management*, *62*(2), 104099.

[14] Nguyen, M., Trinh, N., Mehrotra, A., & Basahel, S. (2025). Generative AI in the workplace: how employee experiences influence work outcomes?. *Journal of Enterprise Information Management*, *38*(5), 1647-1666.

[15] Jo, H., & Park, D. H. (2024). Effects of ChatGPT's AI capabilities and human-like traits on spreading information in work environments. *Scientific Reports*, *14*(1), 7806.

[16] Retkowsky, J., Hafermalz, E., & Huysman, M. (2024). Managing a ChatGPT-empowered workforce: Understanding its affordances and side effects. *Business Horizons*, *67*(5), 511-523.

[17] Feng, C. M., Botha, E., & Pitt, L. (2024). From HAL to GenAI: Optimizing chatbot impacts with CARE. *Business Horizons*, *67*(5), 537-548.

[18] Ossadnik, J., Muehlfeld, K., & Goerke, L. (2023). Man or machine–or something in between? Social responses to voice assistants at work and their effects on job satisfaction. *Computers in Human Behavior*, *149*, 107919.

[19] Syamfithriani, T. S., Wibisono, Y., Munir, M., Wibowo, L. A., & Rahayu, A. (2024, June). Systematic Literature Review: The Role of Enterprise Architecture in Digital Transformation in the Era of the Fourth Industrial Revolution. In *8th Global Conference on Business, Management, and Entrepreneurship (GCBME 2023)* (pp. 418-425). Atlantis Press.

[20] Tojib, D. R., Sugianto, L. F., & Sendjaya, S. (2008). User satisfaction with business-to-employee portals: conceptualization and scale development. *European Journal of Information Systems*, *17*(6), 649-667.