

Safe and Sound:

How Enterprise Request Management Improves Process Efficiency While Reducing Security Risks

Enterprise request management (ERM) is a service delivery strategy that combines a single intuitive Web portal with a workflow automation software engine to automate and accelerate fulfillment processes across an enterprise. Customers (internal or external) can request any type of service, resource, or equipment, as well as check on the status of pending requests, from a single point of entry.

Not only do customers benefit via an improved experience and ease of use, but there are also substantial benefits to the organization from a business perspective. Those benefits include:

- Increased process efficiency via centralization and standardization of delivery;
- Improved employee productivity;
- Faster fulfillment of customer requests, equating to happier customers;
- Service delivery cost reduction through automation; and
- Improved alignment with corporate compliance through reduction of manual, human-based tasks.

This document explains how an ERM approach improves service while lowering risk by improving not only processes related to Identity and Access Management (IAM), but also facility and security access. For more information on ERM, please visit www.erm.info.

Visibility, Control and Efficiency

Effectively managing access to key corporate resources is a continuously evolving battle in today's large enterprise. Organizations need not only to manage access to corporate and personal data, intellectual property, and customer information, but also to ensure safe and secure access to physical assets, facilities, and people.

More often than not, the processes supporting various "entry points" to these key resources are managed within functional silos. Access governance is divided across multiple shared service groups (HR, facilities, IT, security), creating the need for multiple fulfillment areas to participate in delivering access. Shared services organizations each utilize their own tools to automate the access provisioning falling into their areas of responsibility. With respect to the enterprise, the siloed delivery model leads to gaps in process consistency, user experience and service levels.

Essentially, due to their size and complexity, corporations, government agencies, and service providers have struggled to implement consistent access controls that are easily manageable for customers and can be automated end-to-end across the enterprise.

Illusions of Safety: A Risk Management Example

Frequently in the news, one hears of corporations dealing with security breaches wherein sensitive data is compromised, creating massive exposure and liability. Leaking of customer, financial, or other sensitive data is costly and damaging to a company's reputation.

Most often, the breach isn't a result of the affected organization not having a mature approach to information security, or the right tools to minimize exposure, but rather to the lack of a true enterprise-oriented approach to the process. The following example illustrates how ERM addresses this.

A healthcare organization (Sithco) engages with a service provider (ACME) to manage the implementation of a new data center. ACME assigns a team to manage and implement the project (building out the data center and infrastructure). The team consists of a project manager, a technical architect, a network administrator, and 10 staff who will perform the physical installation.

Before the project begins, all of the people on the ACME team must pass background checks in order to be provided with approved access to key resources:

- Sithco's corporate time-keeping system (managed by HR)
- The physical data center location to do the build (managed by facilities)
- The Sithco corporate project management system (managed by the IT PMO)
- Corporate email address and IDs for network access (managed by IT security)

For compliance purposes, as well as alignment with Sithco's corporate security and risk management policies, each shared service group defines its own process and procedures, based on its requirements. This includes the use of tools for fulfillment automation and compliance reporting.

HR uses Peoplesoft® for task assignments. IT uses an enterprise identity management (IDM) solution to manage entitlements and network IDs, as well as an ITSM platform for ticketing. Facilities processes are handled manually via email. For physical facility access control, Sithco has implemented a smart card system that manages access and provides reporting.

From a corporate security and compliance point of view, these defined best-practices align to corporate policy and minimize risk. *Or do they?*

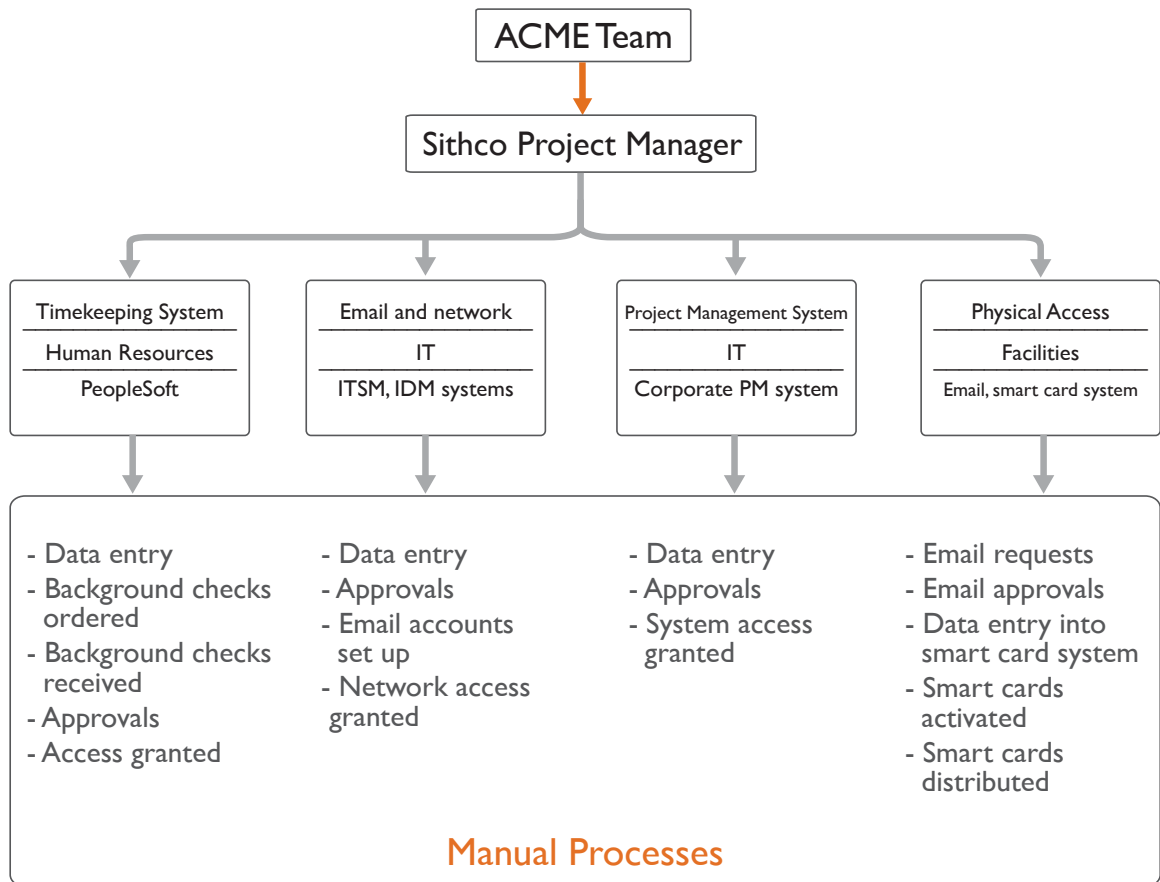
Hidden Complexity in “Straightforward Processes”

Assuming that all security clearances and approvals are completed prior to the project start date, the ACME team will begin the project on time and be productive while adhering to the security policies Sithco has in place. *Is this effective? Possibly. Is it efficient? Probably not.*

Sithco has invested energy into reducing risk and ensuring that access to systems, facilities, and data is governed in line with corporate and legal requirements. From the perspective of each of the shared services groups (HR, facilities, IT, etc.), these access control processes seem straightforward. However, they are more complex when viewed from the vantage point of the enterprise.

In the scenario described above, when the project begins, the Sithco manager overseeing the implementation needs to ensure that every member of the project team has been granted the appropriate access rights, or else they may face lost productivity and project delays. The provision of both physical and IAM access is broken into disparate fulfillment steps across multiple back-end systems, people, and processes.

Specifically, the project security access process entails multiple service requests to fulfillment groups (HR, facilities, IT, etc.) and input of data into multiple systems, along with manual steps (e.g., facilities responding to email requests for smart card access and HR ensuring that background checks are executed properly by a third-party provider).



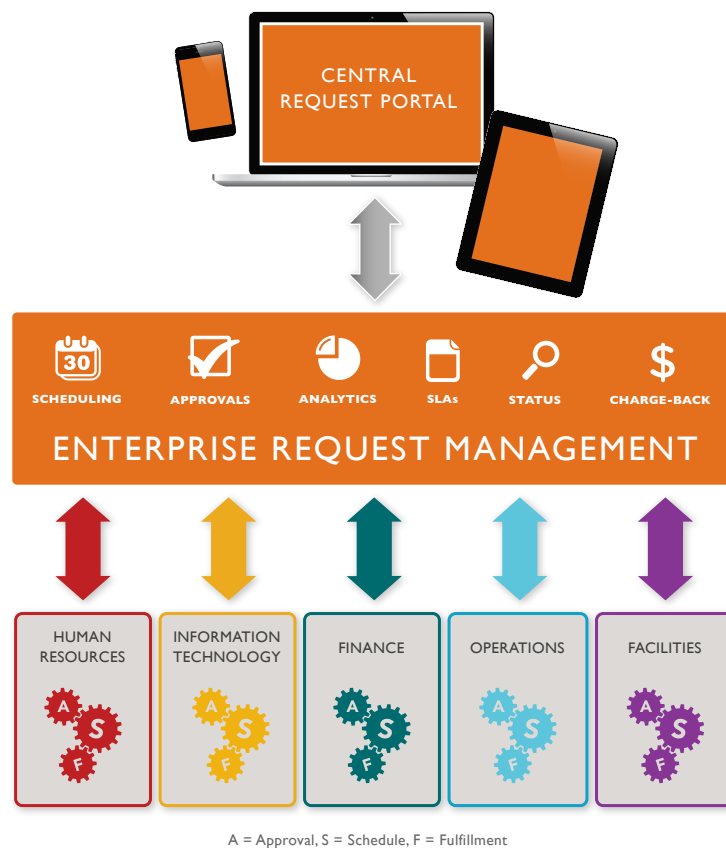
Likewise, when the project ends, the project manager needs to arrange deprovisioning of security access for the ACME team as well, which is equally complex.

While each of Sithco's fulfillment groups have effectively implemented access control best practices, from an enterprise perspective, there is both a loss of corporate efficiency as well as newly created security gaps due to lack of a centralized process. This scenario, while generic, is unfortunately common.

Enterprise Request Management: Higher Efficiency, Lower Risk

Enterprise request management (ERM) is a service delivery strategy that offers fully integrated business process automation, delivered in a customer-centric user interface and employing an integrated back-end delivery model. The goal of an ERM strategy is to allow business service providers to meet enterprise service delivery requirements for shared-service environments in a scalable, cost-effective manner.

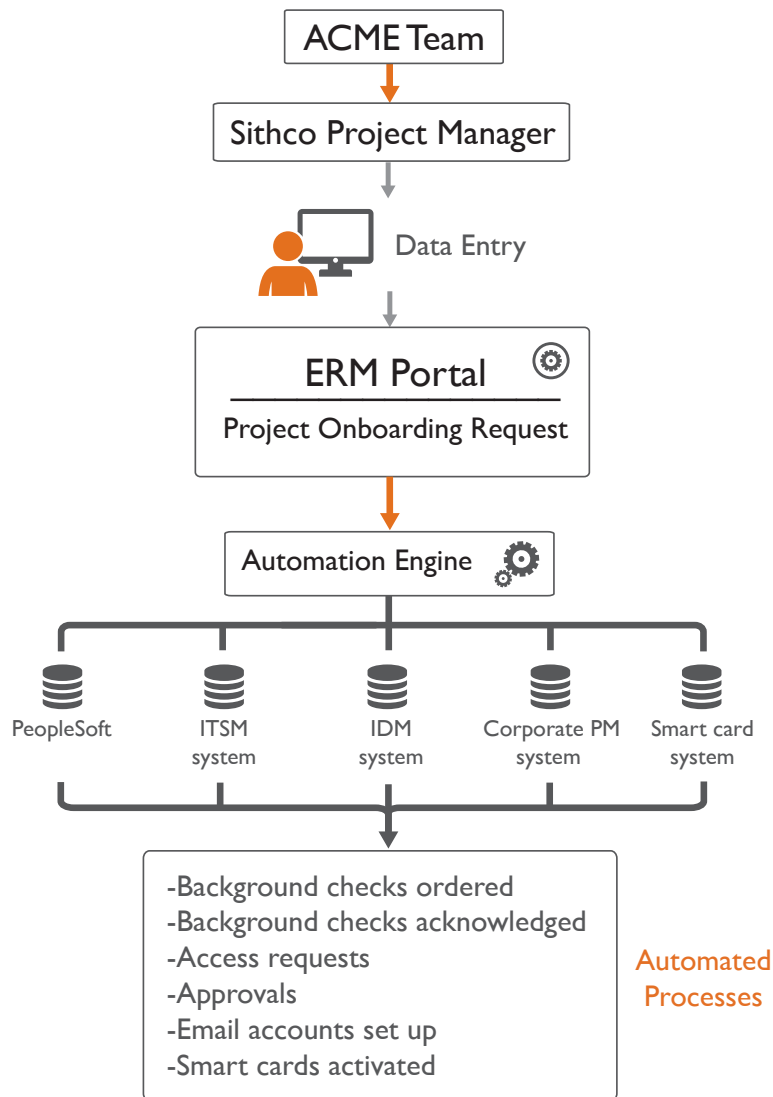
In this collaborative approach, a single, easy-to-use request portal (a.k.a. a system of engagement) replaces the hodgepodge of emails, phone calls and disparate department online request form front-ends. And an automated task management “backbone” application eliminates siloed functions and manual processes by automatically managing approvals, scheduling, and fulfillment through secure communications with and between departmental software platforms (systems of record).



In the example above, employing an ERM approach would not only reduce risk and security exposure for Sithco, but would also improve corporate efficiency by utilizing a centrally governed access management framework.

Upon contract approval, The Sithco project manager would navigate to the project onboarding request screen on the ERM portal. He or she would input the data relevant to the project, and the system would then automatically coordinate all of the security-access-provisioning steps, including notifications, approvals, and status updates.

In this approach, once the data is entered up front—one time, in one place—the defined enterprise delivery model is automated end-to-end, including orchestration of all the existing access-control steps in departmental fulfillment systems. Centralizing this process at the enterprise level not only reduces risk by creating a true end-to-end access governance model, but also allows for key shared service groups to manage and maintain their specific fulfillment models in a distributed manner. The result is *not only a more effective process, but also a more efficient one.*



The decommissioning process at the conclusion of the project is likewise automated.

Summary

Effectively managing both digital and physical security, as well as access to corporate resources, is challenging in a constantly evolving organization. In many enterprises, security is managed within functional silos. While each functional group may be utilizing best practices from a departmental perspective, the result of this approach is inefficiency and increased risk for the organization as a whole.

Enterprise request management (ERM) is a business efficiency strategy that combines a single, intuitive Web portal for requesting any type of enterprise service or resource with back-end process automation. ERM is an ideal alternative to siloed processes for enterprise security and access management, as it eliminates the need for redundant data entry and automates back-end approval and fulfillment processes.

Because it centralizes service request management, ERM enables the coordination of tasks in complex processes (such as providing temporary access to corporate facilities and systems to an outside vendor) that cross functional boundaries. It improves efficiency through automation and elimination of duplicate efforts, while increasing effectiveness by ensuring that all required tasks and approvals are completed.

How Kinetic Request and Kinetic Task Support ERM

Kinetic Request is a powerful and flexible enterprise-wide request management portal application. Coupled with Kinetic Task, it provides the foundation for an ERM system that automates business processes end-to-end across an enterprise.

Kinetic Request enables organizations to implement an effective ERM strategy that is scalable, flexible and manageable. Users can request any type of service or resource using an intuitive Web portal, without training. It's common for companies to build enterprise service catalogs that offer services from all internal groups (IT, HR, facilities, payroll, security, finance), as well as services that cross functional boundaries (such as employee or project onboarding), from a single portal.

Kinetic Task is an advanced workflow automation engine that can communicate with virtually any enterprise data source, and empowers business process owners to design active task trees using graphical tools. It provides workflow orchestration via secure communication with core enterprise management systems and department applications (ITSM, HRMS, CRM, payroll, Active Directory, and custom systems) using common integration techniques such as SOAP and REST.

Kinetic Task enables nontechnical users, with minimal IT assistance, to design and automate simple or complex task workflows and fulfillment processes, while centralizing business approvals and notifications.

About Kinetic Data

Kinetic Data has helped hundreds of Fortune 500 and government customers—including General Mills, Avon, Intel, 3M, and the U.S. Department of Transportation—implement business service management and enterprise request management (ERM) applications aligned with ITIL best practices. Kinetic Data was named “Innovator of the Year” by an independent group of enterprise software users, and the company has also been recognized with awards for its superior customer service and support. Kinetic Data serves customers from its headquarters in St. Paul, Minn., offices in Sydney, Australia, and through a network of reseller partners.

For more information, visit www.kineticdata.com.

PeopleSoft is a registered trademark of Oracle Corporation and/or its affiliates.