(855) 722-5700
info@infobelt.com
infobelt.com

Application Retirement

THE PRACTICAL GUIDE FOR LEGACY APPLICATION MAINTENANCE

Contents

The Problem of Supporting Legacy Applications

Most companies have at least one legacy application they still support just because they need its data, and some organizations have hundreds of legacy applications. Legacy applications are no longer being updated with live data because they have been divested, replaced by next-generation platforms, or are no longer needed.

While most legacy applications cannot be decommissioned because they contain valuable business data, that same data may have retention requirements for operational or compliance purposes. Discarding an irreplaceable wealth of historical information that may deliver essential business information might be considered too risky of an endevour.

No matter the reasons for keeping legacy applications, the risk and problems associated with holding on to unused applications cannot be ignored. High costs and expensive overheads, and antiquated security and access methods expose the information to potential breaches and may impact customer service. Also a shortage of IT personnel with the skills needed to maintain legacy systems increases business risk. Application retirement offers a solution.

What Is Application Retirement?

Application retirement is the process an organization can use to decommission applications and any supporting hardware or software while securely keeping the data accessible to maintain business continuity.

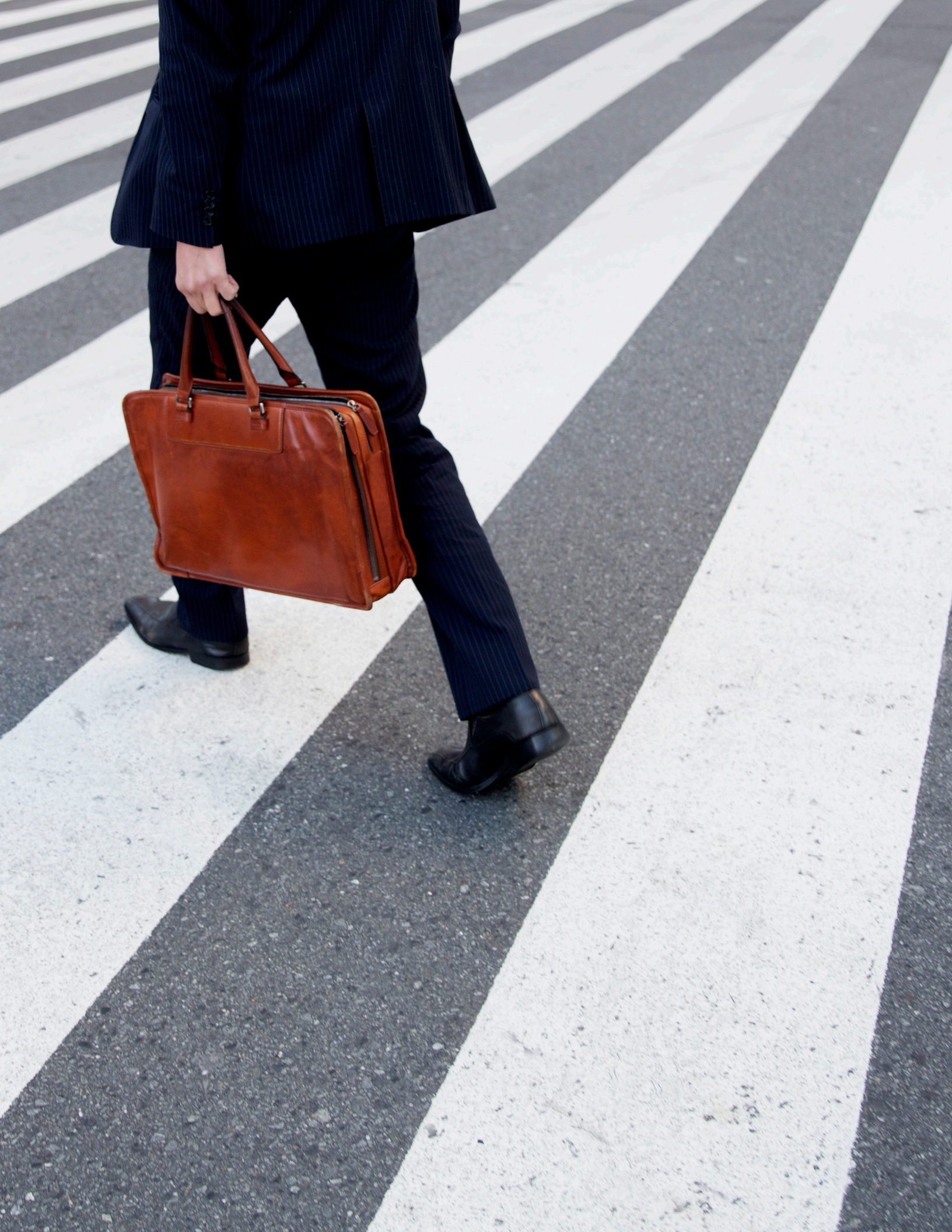
An application retirement program relies on technology, a thorough process, and in-depth knowledge of the business. Any application retirement program must ensure that the right data is retained and in the correct business context so that the data remains meaningful to business users long after the legacy application is decommissioned.

The Benefits of Application Retirement

No two retirement projects are the same. The drivers, solutions, and benefits will vary according to the nature of the legacy application and the organization's priorities.

There are three main benefits that any application retirement program should deliver:

- ✓ Direct savings through the elimination of legacy support and maintenance costs
- ✓ Efficiency gains by delivering effortless access to historical business data
- ✓ Regulatory compliance through application retention rules manages data securely throughout its lifecycle



The Drivers for Application Retirement

As a result of typical business and IT operations, applications regularly become redundant.

Examples can include:

- Mergers and acquisitions creating duplicate applications
- Certain business functions ceasing to operate or being divested
- Applications being replaced with more up-to-date alternatives such as ERP systems

Original applications may be outdated or not needed anymore; some or all of the data created by the application is usually required by the business for analysis or regulatory compliance purposes. However, moving all of the historical data to a live replacement application usually isn't practical because of the adverse impact on system performance, additional costs, and technical difficulties converting the data from the original application. If another alternative solution isn't found, the organization will have to maintain access to the data. Ultimately problems may start to mount up and become powerful drivers for decommissioning or retiring the legacy application.

The Drivers for Application Retirement

Business Risks

People with technical skills required to maintain a legacy system are in short supply, but if those with these skills happen to be available to you, their expertise could be very costly. It's also not uncommon for the people familiar with the original application to have left the organization, which increases the risk of significant delays when a system problem arises. What's worse an issue may come up that proves unfixable, and access to the application data is completely lost. Legacy applications may only work with older operating systems and databases that have not had security patches or updates, which increases the probability of data leaks and other cybersecurity risks.

The Need for Innovation

Supporting legacy systems is a distraction from modern business and IT initiatives. Retiring legacy applications not only frees IT personnel from firefighting problems on systems that have little value to the company but also reduces the overhead needed while allowing the IT team to focus its energy on innovation.

Rising Costs

Software and hardware maintenance and data center costs can add up to 75% of an organization's IT spending, making supporting a legacy application to view historical data very expensive. In some instances, software vendors will charge more for supporting older versions. IT personnel's extra time resolving problems associated with less familiar systems can also create high support costs.

Compliance Concerns

Around the world, there is rising concern about data governance. Regulations such as SEC 17a-3, SEC 17a-4, FINRA 4511, GDPR, and many other government mandates have forced companies to pay closer attention to managing data and protecting data privacy. Older applications may not provide the security levels required to control sensitive data access and may be incompatible with modern access requirements.

Businesses must also balance the two priorities of data minimization and compliance with long-term retention requirements. A legacy application typically lacks the necessary controls to meet these requirements. In contrast, a purpose-built application retirement repository will incorporate information lifecycle management capabilities to handle data retention, data destruction at the end of life, eDiscovery, and legal holds.

The Customer Experience

Legacy systems are isolated from the new applicants that have replaced them, severing the connectivity to their data. Customer requests can be slower and less efficient if customer service teams log into multiple systems to access customer information. Maintaining seamless customer service following mergers and acquisitions is challenging, primarily when pre-and-post merger data is held in two or more systems.

A single content repository for legacy and current application data provides secure access to all information in one place. Such a repository can be integrated with core business applications to create a single point of information for the customer support team looking for a record of all interactions with each customer. This will improve customer service and create a personalized experience for your customers.

Business Intelligence

Most organizations have a stockpile of operational and customer data hiding in legacy systems that adds up to years or even decades of priceless information that could deliver valuable business intelligence, but only if it's easy to access. Decommissioning or retiring an application offers a way to bring together diverse information from disparate systems into a single location. Once combined, the data can be mined using analytical tools or integrated using artificial intelligence.

End-User Experience

Many legacy applications pre-date modern access methods and are frequently challenging to integrate with other platforms. Moving data to a single content repository with a built-in web interface allows business users and auditors to retain access to that data. Decommissioning an application provides an enhanced user experience without developing a bespoke application internally. Modern integration mechanisms also permit easier integrations with other third-party applications.

Building the Business Case

Often the most challenging part of a retirement program is getting it off the ground. It can be challenging to know where to start for organizations considering to retire legacy applications for the first time.

Here are the initial steps:

STEP 01

Get Leadership Buy-In

There are many essential steps to take, but the first step is to have leadership buy-in. It helps to have a senior business or IT executive take ownership of the initiative.

STEP 02

Build a Decommissioning Team

The second most crucial step is to engage the business stakeholders using or owning the application data. The key to the success of any decommissioning project is to build a decommissioning team that includes representatives from the business, compliance, and IT teams. A representative from these business functions will be in the best position to explain how the legacy application is being used and what information will be needed from them in the future, either from a business standpoint or because of a regulatory mandate, and at what frequency.

STEP 03

Design Critieria for Assessments

Once a decommissioning team has been identified, the third step is for the team to design the criteria an application has to meet to remain active.

STEP 04

Classify Applications

Next, the group must classify applications based on the agreed standards. This will help to build a compelling business case and prioritize those applications where decommissioning will deliver the greatest return.

Help in Classifying Applications

Infobelt has developed criteria we recommend our clients use to classify and prioritize which applications to retire. Our standards are based on over 60 years of working inside some of the world's largest financial services firms. We have also conducted thousands of successful decommissioning projects after mergers and acquisitions, divestitures, and hardware/software upgrades.

(See sidebar on the right.)

As part of the business case, we recommend that the decommissioning team build a roadmap of the potential applications to be retired and when to retire them while assessing the benefits and costs associated with decommissioning those applications.

Example Criteria:

TIMING
Is there an event like a divestiture approaching?

TECHNICAL RISK
How will technical problems or resourcing issues impact the business or regulatory mandates?

BUSINESS RISK
How will regulatory requirements, business operations, and customer support be impacted?

HARDWARE AND SOFTWARE COSTS
What are the actual costs of running the application, its underlying infrastructure, and what can be eliminated?

USAGE
How many business users need access to the application, how often, and what for?

Evaluating Application Retirement Plans

Key Requirements

Following a methodical process and using appropriate technology is needed to ensure business continuity for every organization embarking on an application retirement program. Any decommissioning solution should meet the following core requirements:

- **Accessibility**
- **Data Reliability and Usability**
- **Data Integrity**
- **Compliance and Information Lifecycle Management**
- **Performance**
- **Risk Management**
- **Low Total Cost of Ownership**
- **Security**

Accessibility

The most prominent challenge organizations will face is ensuring that internal business end-users and external users, such as regulators, still have access to that data from an application being retired. Any historical information frequently accessed as part of core business processes should be handled with the highest levels of care and not be negatively affected.

An application retirement solution must allow the end-users to obtain the same information they currently get from the application as quickly as they do today, or preferably with more ease. Application programming interfaces (APIs) should be available to enable integrations with other applications.

Data Reliability and Usability

Many business applications apply calculations, logic, and other business rules to application data as part of the end-user experience. For example, a database table with a status code "1" might be displayed on the screen as the word 'active.' A database table with a status of "2" may be displayed as the word "closed." Understanding and applying these status codes is critical to ensure that the data will constantly be recreated accurately and in a meaningful way when the data is accessed. To avoid additional risks to the business and avoid relying on users or IT personnel with detailed data model knowledge, capturing all application logic during the decommissioning process is a must. The repository you choose to maintain the application data in should be accessible for authorized users to navigate quickly, without high levels of technical skills, prior experience with the legacy application, and without the help of IT.

"The Great Resignation" and high staff turnover have also shown that the data must be presented in context to make it self-explanatory. An easy-to-use self-service portal with pre-built queries and searches will help support customer service teams and regulators when they need to find specific information and data.

Data Integrity

To remain compliant with regulatory mandates and ensure accurate records, it is essential that data extracted from a retired application cannot be changed once it has been decommissioned. Any solution should provide tamper-proofing measures or WORM (write once read many) technologies at the software and hardware level. Ensuring the integrity of your data will not only keep you compliant but also help protect your business' reputation.

Evaluating Application Retirement Plans

Key Requirements (continued)

Compliance and Information Lifecycle Management

Many regulatory mandates require data to be retained for specific periods and destroyed at the end of its valuable and legal lifetime. This is also a good business practice that organizations should implement in their business continuity plans. Whatever decommissioning solution an organization chooses should reinforce corporate data retention policies and allow information to be accessed and preserved. We recommend that the retirement solution also have eDiscovery, automated retention periods, legal holds, and automated defensible destruction capabilities. This will help minimize data storage needs, fulfill regulatory obligations, and reduce the risk of regulatory exams or legal investigations.

Performance

Typically, access to historical data also reduces over time, but immediately after decommissioning, the application data may need to be accessed regularly by business users. Therefore, any solution should be scalable, up and down, to handle the changes in storage and access requirements. If an organization needs to or wants to retire more than one legacy application, it should select a repository that can support structured and unstructured data. It should also have data compression capabilities to provide savings in storage space.

Risk Management

One of the most common reasons organizations defer decommissioning initiatives is the perceived risk of losing data or disrupting business activities. These risks can be managed simply by following an effective decommissioning process. What's more important for companies to focus on is the risk associated with applications and systems with outdated security parameters housing clients' personal and financial information. A massive data leak or ransomware attack can damage a company's reputation beyond repair and cause major regulatory problems that could hamper business growth for years.

Low Total Cost of Ownership

The long-term cost reduction of any decommissioning project is a realistic and achievable goal. Companies spend a significant portion of their IT budget on maintenance alone, so eliminating the licensing and maintenance costs of the legacy application will minimize the ongoing cost of retaining the application data in four key areas:

- **Hardware**
- **Software**
- **Services**
- **Environmental**

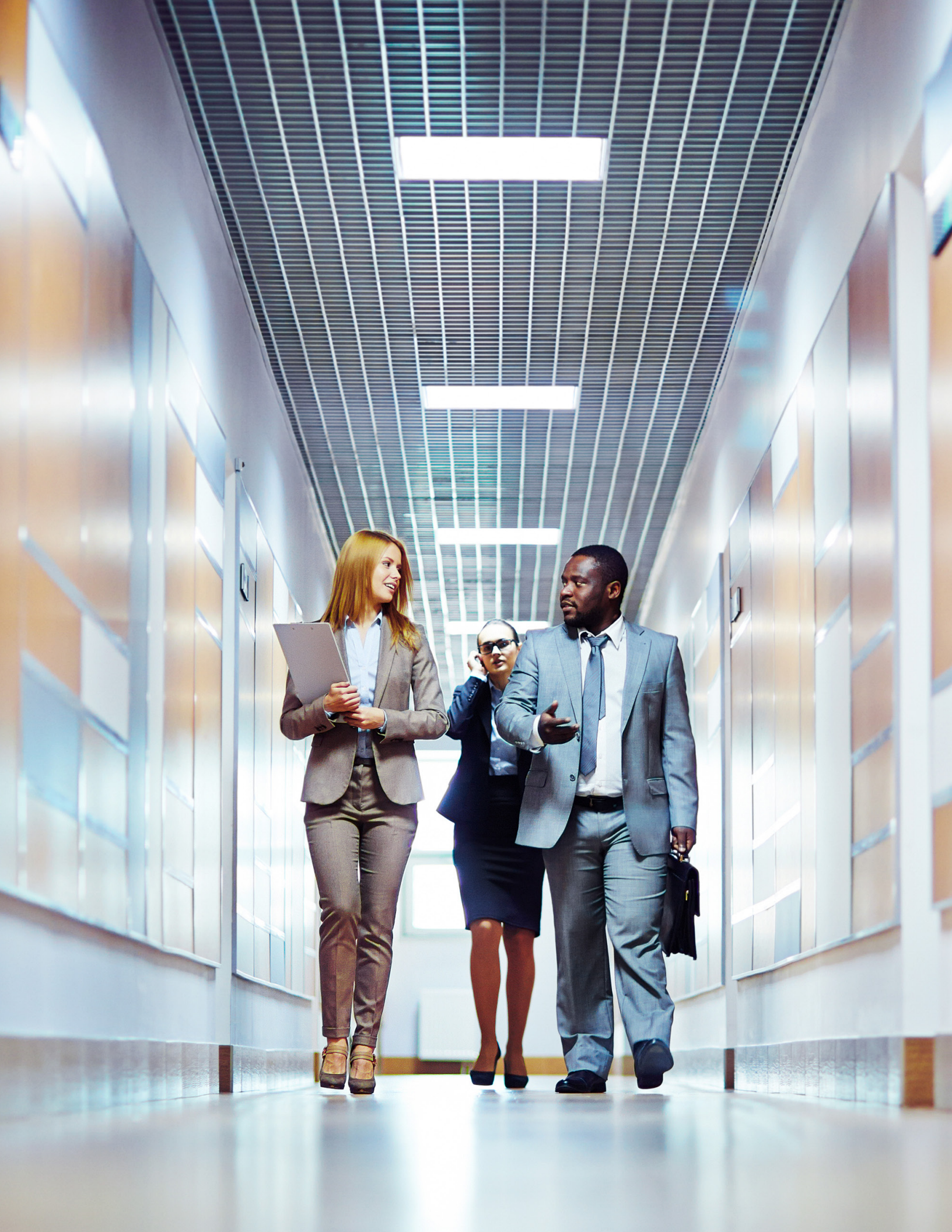
Security

There are three key security considerations that should be considered when choosing an application retirement technology:

User authentication—Preventing unauthorized access to legacy data by deploying multi-factor authentication to confirm the identity of system users.

User fine-grained entitlements—Protecting data by restricting access to different categories and subsets of data by individual users and groups.

Data security—Ensuring the data is secured using encryption and WORM storage, sometimes employing Zero-Trust methodology.



The Infobelt Approach

The Infobelt Omni Archive Manager (OAM) **Application Retirement Workbench** uses an eight-step process to ensure business continuity by incorporating all business needs for using the application data into the final decommissioning solution. No previous business application knowledge will be needed to use or support the system in the future.

Our OMNI Archive Manager repository is the final resting place for the retired application data. OAM can store structured and unstructured data from any application running on any platform. This means you can store transactional data, websites, emails, documents, images, videos, and even chats all in one place.

Our eight-step process includes:

STEP 01	Business Analysis
STEP 02	Systems Analysis
STEP 03	Data Extraction
STEP 04	Data Processing
STEP 05	User Access Design
STEP 06	User Acceptance Testing
STEP 07	Data Transfer
STEP 08	Application Retirement

The Infobelt Application Retirement Process

Step by Step

STEP 01 Business Analysis

Infobelt evaluates the client's business requirements and understands the uses for the data, such as:

- Which data needs to be retained, and for how long?
- How users work with the application and how they navigate between screens.
- What queries or reports do users run to obtain information from the application?

STEP 02 Systems Analysis

System analysis defines the technical scope of the tasks, including the location and formation of the data, which could exist in a range of structured formats like data files and database tables, as well as unstructured formats like documents, and rich media files. Any business rules for processing the data are also identified, which are applied in step four below.

STEP 03 Data Extraction

Data from the legacy system is extracted to meet the business's data retrieval and compliance needs. This may include historical transactional data in database records and documents such as invoices. Redundant or system-only data is not extracted to minimize storage requirements.

STEP 04 Data Processing

In cases where an application applies business logic to the underlying data to display more meaningful information to the user, for example, translating code into work or calculating totals, these business rules are applied during the data processing stage. This ensures that users understand what they see on the screen without prior knowledge.

STEP 05 User Access Design

There are two options for creating visual layouts for the data.
1. Data View—If business users only rarely access the application data, it is often sufficient for it to be displayed in standard, human-readable formats such as lists and tables.
2. Document View—Content already pre-formatted, such as documents, websites, images, and videos, can be stored in its original format, with no further processing required and accessed alongside application data in the same system.

STEP 06 User Acceptance Testing

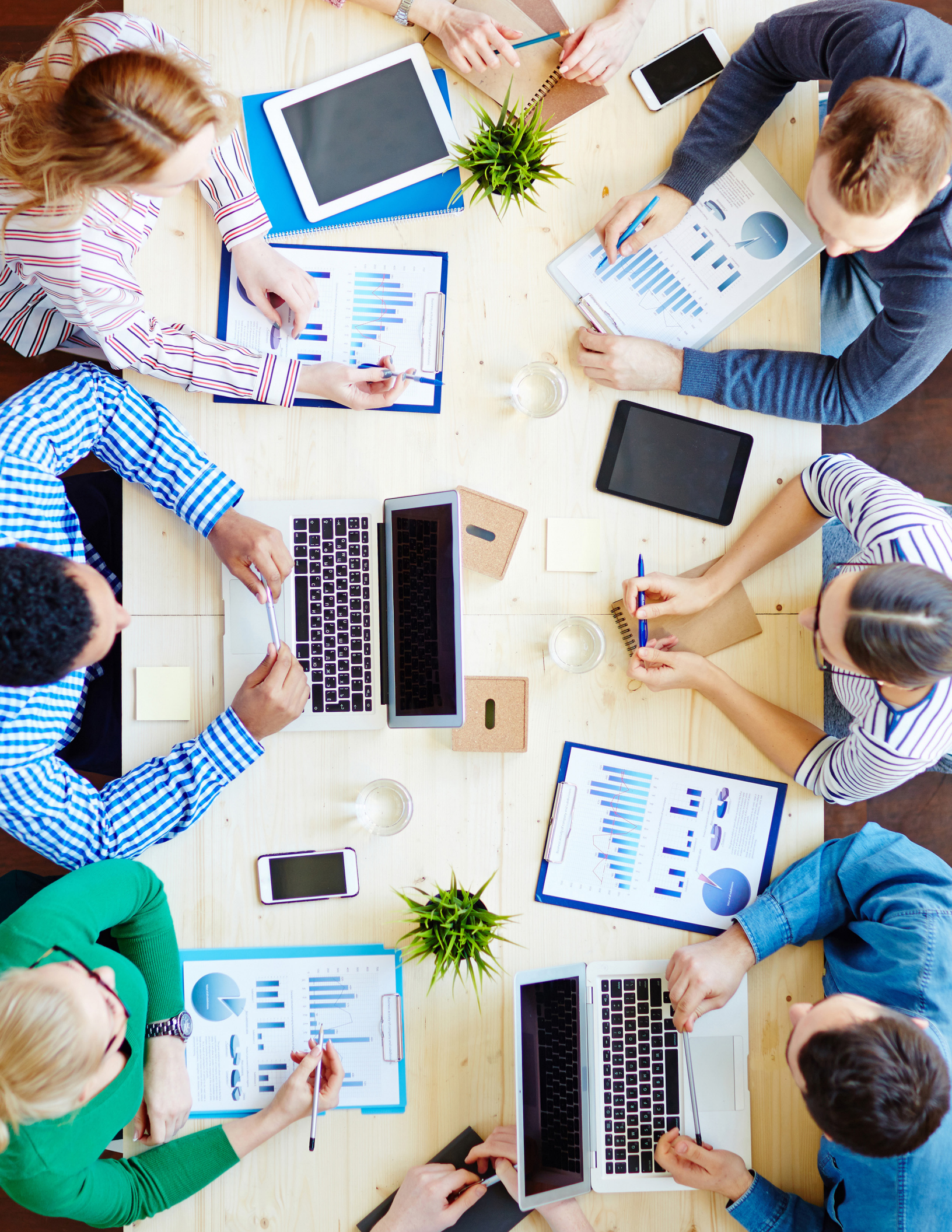
A test system is created using sample data and tested by business users who work through typical scenarios, searching for information using various selection criteria to ensure they can easily access all the information they need.

STEP 07 Data Transfer

On completing user acceptance testing, all the application data is processed to create meaningful outputs, which are then compressed, indexed, and transferred to our OAM repository. The information is stored in WORM format, with appropriate retention rules and access permissions. The repository can be accessed directly for ease of use.

STEP 08 Application Retirement

Once the data has been transferred to the OAM repository, the original application can be retired, together with any supporting hardware and software, allowing the organization to realize the benefits identified in the business case.



How Infobelt Meets the Key Application Retirement Requirements

Our solution has been designed to meet all business requirements for successful decommission identified earlier in this document.

Accessibility

Business users can continue to retrieve information easily as all enterprise data from all decommissioned applications is available in one place. The OAM repository can be accessed using its web interface. At the same time, standard APIs allow third-party applications to access historical data seamlessly, without users needing to log into an operating system.

Data Reliability

Any business logic required to present information to the user in a meaningful form is logically embedded in the stored data. This eliminates the risk of losing the ability to understand, interpret, and correctly use the data if application or data knowledge is lost from the business in the future.

Data Integrity

All information from the decommissioned application is held in a secure, access-controlled, WORM format with no opportunity to tamper with the data.

How Infobelt Meets the Key Application Retirement Requirements (continued)

Usability

OAM is simple and intuitive to use. Presenting data in a meaningful business context ensures that no additional application knowledge or training will be required.

Compliance and Information Lifecycle Management

OAM has an integral information lifecycle management capability that ensures compliance with data retention requirements, including legal holds through the application of retention rules.

Performance

The OAM repository is an enterprise-scalable product with multiple data records, documents, images, and other data types. Efficient data compression rates eliminate redundancy and permit highly efficient storage and access. Robotic process automation helps scalability with large data sets.

Risk Management

The Infobelt OAM Application Retirement Workbench minimizes risk and ensures continuity by focusing on the information requirements of business users. This approach also avoids the need for long-term access to legacy IT skills or application knowledge. The exact process has been used successfully by companies worldwide to decommission vast ranges of bespoke and packaged software applications.

Low Total Cost of Ownership

Infobelt's agile and repeatable process is designed to complete decommissioning projects quickly. Combined with a cost-effective model and lightweight architectural footprint, this delivers a rapid investment return and low total cost ownership. Due to efficient performance, a single OAM instance will typically meet an organization's entire decommissioning requirement. Data from thousands of decommissioned applications can be housed in low-cost WORM storage. As with all major hardware platforms, it is also possible to save additional costs by repurposing the newly freed up hardware.

Security

User Authentication

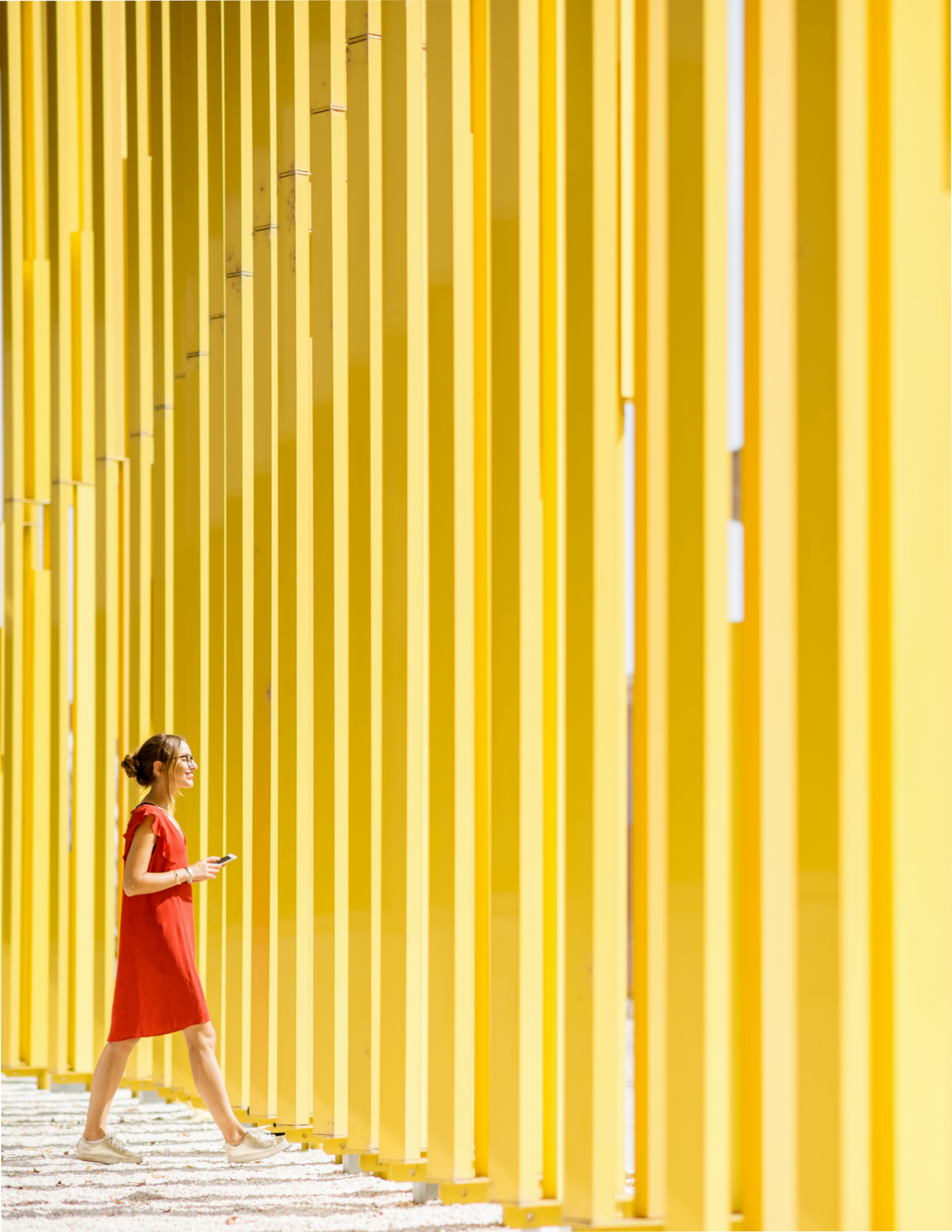
OAM handles user authentication through its in-built security model and integrates enhanced security mechanisms such as multi-factor authentication and encryption.

User Access Rights

Access can be tightly controlled for different users and groups, down to individual field levels, via the fine-grained entitlement feature.

Data Security

The decommissioned data is stored in a compressed WORM format as standard.



The Infobelt Difference

Infobelt has over 60 years of experience in business, technology, and regulatory mandates within large financial services firms.

We bring our regulatory compliance and technology expertise together and work shoulder to shoulder with your team to operationalize processes and solutions that solve the problems that you have today at a cost that's much more competitive than a more prominent consulting or technology firm. The Infobelt Omni Archive Manager repository currently holds over 20 trillion regulated business records from one customer installation. With Infobelt, you get more experience than that of a team from a big four consulting firm and the highest quality of work that can be operationalized to solve your problems at a fraction of the cost.

Ready to Get Started?

CONTACT US :

(855) 722-5700
info@infobelt.com
www.infobelt.com

OUR OFFICE :

428 E. 4th St, Suite 407, Charlotte, NC 28202.

Tame Data. Control Risk.